ThinPrint®Reader

TPR-10

User Manual

Manufacturer:
SEH Computertechnik GmbH
Suedring 11
33647 Bielefeld
Germany
Phone: +49 (0)521 94226-29
Fax: +49 (0)521 94226-99
Support: +49 (0)521 94226-44
Email: info@seh.de
Web: http://www.seh.de

Document:
Type: User Manual
Title: ThinPrint®Reader
Version: 1.1

Online Links to Important Websites:

Support Contacts & Information: http://www.seh-technology.com/support
Sales Contacts & Information: http://www.seh-technology.com/sales
Downloads: http://www.seh-technology.com/services/downloads/tpr.html

InterCon is a registered trademark of SEH Computertechnik GmbH.

SEH Computertechnik GmbH has endeavored to ensure that the information in this documentation is correct. If you detect any inaccuracies please inform us at the address indicated above. SEH Computertechnik GmbH will not accept any liability for any error or omission. The information in this manual is subject to change without notification.

All rights are reserved. Copying, other reproduction, or translation without the prior written consent from SEH Computertechnik GmbH is prohibited.

© 2012 SEH Computertechnik GmbH

All trademarks, registered trademarks, logos and product names are property of their respective owners.

Table of Contents

1 General Information. 5

1.1 ThinPrint®Reader 6
1.2 Documentation. 8
1.3 Support and Service 10
1.4 Your Safety 11
1.5 First Steps 12
1.6 Saving the IP Address in the TPR 13

2 Administration Methods 17

2.1 Administration via the TPR Control Center 18
2.2 Administration via the InterCon-NetTool 20
2.3 Administration via Email 22
2.4 Administration via the Status/Reset Button of the Device 24

3 Network Settings 25

3.1 How to Configure IPv4 Parameters 26
3.2 How to Configure IPv6 Parameters 28
3.3 How to Configure the DNS 30
3.4 How to Configure SNMP 31
3.5 How to Configure POP3 and SMTP 32
3.6 How to Configure Bonjour 35
3.7 How to Configure the Device Time 36

4 Device Settings 38

4.1 How to Determine a Description 38
4.2 How to Configure the Communication between the TPR and the Printer. 38
4.3 How to Define Local Service Ports 40
4.4 How to Use the Notification Service 41

5 Personal Printing Settings 43

5.1 How to Define the Personal Printing Server 44
5.2 How to Encrypt the Connection to the Personal Printing Server 45
5.3 How to Verify the Identity of the Personal Printing Server 46
5.4 How to Configure the Personal Printing Printer 47

6 ThinPrint Settings 49
6.1 How to Define the ThinPrint Port 50
6.2 How to Define the Bandwidth 50
6.3 How to Embed the Printer 51
6.4 How to Define Timeouts 53
6.5 How to Get Status Information on the Printer Connection 54
6.6 How to Get Printer Messages 56
6.7 How to Use the ThinPrint Connection Service 57
6.8 How Does the TPR Receive Encrypted Data? 59

7 Security 60
7.1 How to Define the Encryption Level for SSL/TLS Connections 61
7.2 How to Control the Access to the TPR Control Center 63
7.3 How to Block Individual Ports 64
7.4 How to Control the Access to the TPR (TCP Port Access Control) 66
7.5 How to Use Certificates Correctly 67
7.6 How to Use Authentication Methods 76
7.7 How to Configure a Device Assignment 82

8 Maintenance 83
8.1 How to Secure the TPR Parameters (Backup) 83
8.2 How to Use a Connected USB Device 85
8.3 How to Reset Parameters to their Default Values (Reset) 87
8.4 How to Perform an Update 90
8.5 How to Restart the TPR 91
8.6 How to Print a Status or Service Page 92
8.7 How to Display the Job History 94

9 Appendix 96
9.1 Glossary 97
9.2 Parameter List 100
9.3 Troubleshooting 120
9.4 List of Figures 123
9.5 Index 124

1 General Information

This chapter contains information concerning the device and the documentation as well as notes about your safety.
You will learn how to benefit from your ThinPrint®Reader and how to operate the device properly.

What information do you need?

- 'ThinPrint®Reader' ⇨🗎6
- 'Documentation' ⇨🗎8
- 'Support and Service' ⇨🗎10
- 'Your Safety' ⇨🗎11
- 'First Steps' ⇨🗎12
- 'Saving the IP Address in the TPR' ⇨🗎13

1.1 ThinPrint®Reader

What is ThinPrint Personal Printing Essentials®?

ThinPrint Personal Printing Essentials® is a software-based technology for secure network printing. ThinPrint Personal Printing Essentials is printer-independent.

Printing is carried out from a client to the printer object '**Personal Printer**'. The print job will be saved to the Personal Printing server. The print job will be printed once the user has successfully authenticated to any network printer that is set up for Personal Printing.

What is ThinPrint®?

ThinPrint® is a software-based technology providing print job compression and bandwidth control for network printing. The data traffic between the application server or the print server and the local printer is reduced considerably and networks are relieved.

The ThinPrint technology enables the transmission of compressed and bandwidth-optimized print jobs within a network. Print jobs are compressed using the server component of the .print technology, the so-called **ThinPrint Engine**. The server sends the compressed print data to a device with the implemented **ThinPrint Client**. This client then decompresses the print data, transferring it to any printer.

Purpose

TPR (ThinPrint®Reader) have been specifically designed for environments with ThinPrint Personal Printing technology. The TPR contains a fully integrated **Personal Printing Client**. Together with the Personal Printing server, the Personal Printing Client allows for the authentication process.

TPR are an authentication hardware that allows you to use network printers as Personal Printing printers independent of printer make and model. To this purpose, one TPR is installed between the network and the printer for every network printer.

Users will print to the Personal Printer print object. They will then authenticate to the TPR by means of a contactless smartcard based on RFID. The Personnel Printing server then sends the print job to the TPR, which forwards it to the printer.

Optionally, you can use the ThinPrint technology with the TPR. The TPR contains a fully integrated **ThinPrint Client**. This ThinPrint Client allows you to receive and decompress print data in ThinPrint environments. A network printer can be quickly and easily embedded into the network by means of the integrated ThinPrint Client.

Features

The ThinPrint®Reader supports the following features (amongst others):

- The connection between the TPR and the Personal Printing server is protected by means of the **Personal Printing SSL/TLS encryption**.
- The feature **AutoConnect** allows you to automatically create the required printer objects for the relevant client on the server. **AutoConnect** will automatically connect all selected printers on the server with a ThinPrint port; provided that templates exist.
- The **ThinPrint Connection Service** allows you to print to ThinPrint clients, that are found behind a firewall, for example. This allows the connection via masked networks as well as the assignment of the relevant print job to the respective end device.
- By means of the **ThinPrint SSL/TLS encryption**, the print data is protected during the transmission and will be decrypted by the ThinPrint clients or gateways before printing.

System Requirements

The TPR has been designed for the use in TCP/IP-based networks. A Personal Printing server must be integrated within the network. The network printers involved must support RAW or socket printing (printing via TCP/IP ports), IPP printing or LPD printing. When using the ThinPrint function, a ThinPrint Server needs to be integrated within the network. If you want to use **ThinPrint** or the **ThinPrint Connection Service**, you need the relevant licenses.

1.2 Documentation

Structure of the Documentation

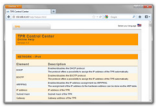
The TPR documentation consists of the following documents:

PDF

User Manual
Detailed description of the TPR configuration and administration.

Printed PDF

Quick Installation Guide
Information about security, hardware installation, and the initial operation procedure.



HTML

Online Help (TPR Control Center)
The Online Help contains detailed information about how to use the 'TPR Control Center'.

HTML

Online Help (InterCon-NetTool)
The Online Help contains detailed information about how to use the software tool 'InterCon-NetTool'.

Document Features

This documentation has been designed as an electronic document for screen use. Many programs (e.g. Adobe® Reader®) offer a bookmark navigation feature that allows you to view the entire document structure.

This document contains hyperlinks to the associated information units. If you want to print this documentation, we recommend using the printer setting 'Duplex' or 'Booklet'.

Terminology Used in this Document

The explanation of technical terms used in this document is summarized in a glossary. The glossary provides a quick overview of technical matters and background information; see: ⇨ 97.

Symbols and Conventions

A variety of symbols are used within this document. Their meaning is listed in the following table:

Table 1: Conventions within the documentation

Symbol / Convention	Description
Warning	A warning contains important information that must be heeded. Non-observance may lead to malfunctions.
Note	A notice contains information that should be heeded.
Proceed as follows: 1. *Mark ...*	The 'hand' symbol marks the beginning of instructions. Individual instructions are set in italics.
Confirmation	The arrow confirms the consequence of an action.
☑ Requirements	Hooks mark requirements that must be met before you can begin the action.
☐ Option	A square marks procedures and options that you can choose.
•	Eye-catchers mark lists.
	This sign indicates the summary of a chapter.
⇨	The arrow marks a reference to a page within this document. In the PDF file, you can jump to this page by clicking the symbol.
Bold	Established terms (of buttons or menu items, for example) are set in bold.
`Courier`	Command lines are set in Courier font.
'Proper names'	Proper names are put in inverted commas

1.3 Support and Service

Support

If questions remain, please contact our hotline. SEH Computertechnik GmbH offers extensive support.

	Monday through Thursday Friday	from 8:00 a.m. to 4:45 p.m. and from 8:00 a.m. to 3:15 p.m. (CET)
	+49 (0)521 94226-44	
	support@seh.de	

Current Services

The following services can be found on the SEH Computertechnik GmbH homepage http://www.seh-technology.com/:

- current firmware
- current tools
- current documentation
- current product information
- product data sheet
- and much more

1.4 Your Safety

Read and observe all safety regulations and warnings found in the documentation, on the device and on the packaging. This will avoid potential misuse and prevent damages to people and devices.

SEH Computertechnik GmbH will not accept any liability for personal injuries, property damages and consequential damages resulting from the non-observance of the mentioned safety regulations and warnings. Non-observance will result in the warranty claims becoming void.

Intended Use

The TPR is used in TCP/IP networks. The TPR is an authentication hardware that allows you to use network printers as Personal Printing printers independent of printer make and model. The TPR has been designed for use in office environments.

Improper Use

All uses of the device that do not comply with the TPR functionalities described in the documentation are regarded as improper uses. It is not allowed to make modifications to the hardware and software or to try to repair the device.

Safety Regulations

Before starting the initial operation procedure of the TPR, please note the safety regulations in the 'Quick Installation Guide'. The Quick Installation Guide is enclosed in the packaging.

Warnings

Read and observe all warnings mentioned in this document. Warnings are found before any instructions known to be dangerous. They are presented as follows:

Warning!

1.5 First Steps

This section provides all the information that you need for a fast operational readiness.

Proceed as follows:

1. *Read and observe the security regulations in order to avoid damages to people and devices, see:* ⇨ 11.
2. *Carry out the hardware installation. The hardware installation comprises the connection of the TPR to the printer, network and the mains supply; see: 'Quick Installation Guide'.*
3. *Make sure that the former IP address of the printer is saved in the TPR and that the printer is set to DHCP; see: 'Saving the IP Address in the TPR'* ⇨ 13.
4. *Define the Personal Printing server and other Personal Printing settings; see:* ⇨ 43.

The TPR is operational.

1.6 Saving the IP Address in the TPR

Why IP Addresses?

An IP address is used to address network devices in an IP network. TCP/IP network protocols require the storing of the IP address in the TPR so that the device can be addressed within the network.

How Does the TPR Obtain IP Addresses?

TPR are shipped without an IP address. The TPR is able to assign itself an IP address during the initial installation. Boot protocols are used to assign an IP address automatically to the TPR. Upon delivery, the boot protocols 'BOOTP' and 'DHCP' are enabled.

Once the TPR is connected to the network, it checks whether an IP address can be obtained via the boot protocols BOOTP or DHCP. If this is not the case, the TPR-10 assigns itself an IP address via ZeroConf from the address range (169.254.0.0/16) which is reserved for ZeroConf.

Once the TPR-10 has automatically received an IP address via a boot protocol, you can save a freely definable IP address in the TPR-10. The assigned IP address of the TPR can be determined and modified via the software tool 'InterCon-NetTool'.

Assign the former IP address of the printer to the TPR-10. Configure the printer to DHCP (if you fail to do so, there will be no functionality).

Different methods for the assignment of the IP address are described in the following.

Automatic Methods of IP Address Assignments

- 'ZeroConf' ⇨🗎14
- 'BOOTP' ⇨🗎14
- 'DHCP' ⇨🗎14
- 'Auto Configuration (IPv6 Standard)' ⇨🗎15

Manual Methods of IP Address Assignments

- 'InterCon-NetTool' ⇨🗎15
- 'TPR Control Center' ⇨🗎15
- 'ARP/PING' ⇨🗎16

ZeroConf

If no IP address can be assigned via boot protocols, the TPR assigns itself an IP address via ZeroConf. For this purpose, the TPR picks an IP address at random from the address range (169.254.0.0/16) which is reserved for ZeroConf.

You can use the domain name service of Bonjour for the name resolution of the IP address; see: ⇨ 35.

BOOTP

The TPR supports BOOTP, which means that the IP address of the TPR can be assigned via a BOOTP server.

Requirements

☑ The 'BOOTP' parameter has been enabled, see: ⇨ 26.

☑ A BOOTP server is available in the network.

If the TPR is connected, it asks the BOOTP host for the IP address and the host name. The BOOTP host answers and sends a data packet containing the IP address. The IP address is saved in the TPR.

DHCP

The TPR supports DHCP, which means that the IP address of the TPR can be assigned dynamically via a DHCP server.

Requirements

☑ The 'DHCP' parameter has been enabled, see: ⇨ 26.

☑ A DHCP server is available in the network.

After the hardware installation, the TPR asks a DHCP server for an IP address by means of a broadcast query. The DHCP server identifies the TPR on the basis of its hardware address and sends a data packet to the TPR.

This data packet contains, among others, the IP address of the TPR, the default gateway, and the IP address of the DNS server. The data is saved in the TPR.

Auto Configuration (IPv6 Standard)

The TPR can have an IPv4 address and several IPv6 addresses at the same time. The IPv6 standard is used to automatically assign IP addresses in IPv6 networks. When connected to an IPv6 network, the TPR will automatically obtain an additional link-local IPv6 address.

The TPR uses the link-local IP address to search for a router. The TPR sends so-called 'Router Solicitations' (RS) to the special multicast address FF02::2. The available router will then return a 'Router Advertisement' (RA) containing the required information.

With a prefix from the range of the globally unique addresses, the TPR can compose its own address. It simply replaces the first 64 bits (prefix FE80::) with the prefix that was sent in the RA.

Requirements

☑ The 'IPv6' parameter has been activated.

☑ The 'Automatic configuration' parameter has been activated; see: ⇨ 28.

To configure the assignment of IPv6 addresses, see: ⇨ 28.

InterCon-NetTool

The InterCon-NetTool has been developed by SEH Computertechnik GmbH for the administration of SEH network devices. The IP Wizard of the InterCon-NetTool helps you to configure the TCP/IP parameters, e.g. the IP address. You can manually enter the desired IPv4 address and save it in the TPR using the IP Wizard. To configure an IPv4 address via the InterCon-NetTool, see: ⇨ 26.

TPR Control Center

You can manually enter the desired IP address and save it in the TPR using the TPR Control Center.

- To configure an **IPv4** address via the TPR Control Center, see: ⇨ 26.
- To configure an **IPv6** address via the TPR Control Center, see: ⇨ 28.

ARP/PING

The assignment of the IP address to the hardware address can be done via the ARP table. The ARP table is an internal system file in which the assignment is temporarily saved (about 15 min). This table is administered by the ARP protocol.

By means of the 'arp' and 'ping' commands, you can save the IP address in the TPR. If the TPR already has an IP address, the 'arp' and 'ping' commands cannot be used to save a new IP address.

However, an IP address from the address range (169.254.0.0/16) which is reserved for ZeroConf can be overwritten by means of the 'arp' and 'ping' commands.

The 'arp' command is used for editing the ARP table. The 'ping' command transfers a data packet containing the IP address to the hardware address of the TPR. If the data packet has been successfully sent and received, the TPR permanently saves the IP address.

The implementation of the 'arp' and 'ping' command depends on the system used. Read the documentation for your operating system.

Requirements

☑ The 'ARP/PING' parameter has been enabled, see: ⇨ 26.

Edit the ARP table:
Syntax: `arp -s <IP address> <hardware address>`
Example: `arp -s 192.168.0.123  00-c0-eb-00-01-ff`

Assign a new IP address to the TPR:
Syntax: `ping <IP address>`
Example: `ping 192.168.0.123`

The separators within the hardware address that are used in this example correspond to the Windows® platform.

2 Administration Methods

You can administer and configure the TPR in a number of ways. The following chapter gives you an overview of the various administration options.

You will get information on when to use these methods and which functions these methods support.

What information do you need?

- 'Administration via the TPR Control Center' ⇨ 18
- 'Administration via the InterCon-NetTool' ⇨ 20
- 'Administration via Email' ⇨ 22
- 'Administration via the Status/Reset Button of the Device' ⇨ 24

2.1 Administration via the TPR Control Center

Which Functions Are Supported?

The TPR Control Center comprises all features for the administration of the TPR.

The TPR Control Center is stored in the TPR and can be displayed by means of a browser software (Internet Explorer, Firefox, Safari).

Requirements

☑ The TPR is connected to the network and the mains voltage.

☑ The TPR has a valid IP address.

Starting the TPR Control Center

Proceed as follows:

1. *Open your browser.*
2. *Enter the IP address of the TPR-10 as the URL.*

↳ The TPR Control Center appears in the browser.

If the TPR Control Center is not displayed, check the proxy settings of your browser.

You can also start the TPR Control Center via the software tool 'InterCon-NetTool'.

Proceed as follows:

1. *Highlight the TPR in the device list.*
2. *Select* **Actions – Launch Browser** *from the menu bar.*

↳ The TPR Control Center appears in the browser.

Fig. 1: TPR Control Center - START

Structure of the TPR Control Center

The available menu items are located in the navigation bar (top). After selecting a menu item (simple mouse click), the available submenu items are displayed at the left. After selecting a submenu item, the corresponding page with its content is displayed (at the right).

You can set the language via the menu item **START**. Simply select the relevant flag.

The manufacturer's contact details and additional information regarding the product are displayed under **Product & Company**. The **Sitemap** provides an overview of and direct access to all pages of the TPR Control Center.

All other menu items refer to the configuration of the TPR. They are described in the Online Help of the TPR Control Center. To start the Online Help, click the icon.

2.2 Administration via the InterCon-NetTool

The software InterCon-NetTool has been developed by SEH Computertechnik GmbH for the administration of SEH network devices (TPR, TPG, print server, etc.). Depending on the network device you can configure various features via the InterCon-NetTool.

Mode of Operation

After the InterCon-NetTool is started, the network will be scanned for connected network devices. The network range to be scanned is freely definable. All network devices found will be displayed in the 'device list'.

You can modify the device list and adopt it to your individual needs. You can mark and configure the devices in the device list.

Installation

In order to use the InterCon-NetTool, the program must be installed on a computer with a Windows operating system. The installation file of the InterCon-NetTool can be found on the SEH Computertechnik GmbH homepage:

http://www.seh-technology.com/services/downloads/tpr.html

Proceed as follows:

1. *Start the InterCon-NetTool installation file.*
2. *Select the desired language.*
3. *Follow the installation routine.*

The InterCon-NetTool will be installed on your client.

Program Start

To start the program, double-click the InterCon-NetTool icon . The icon is found on the desktop or the Windows start menu.
(Start --> All Programs --> SEH Computertechnik GmbH --> InterCon-NetTool)

The settings of the InterCon-NetTool are saved in the 'NetTool.ini' file. The file is stored in the directory 'Documents and Settings' with the relevant user name.

Structure of the InterCon-NetTool

After the program start you will see the main dialog with the following elements. The dialog may vary, depending on which elements you have chosen to be shown or hidden.

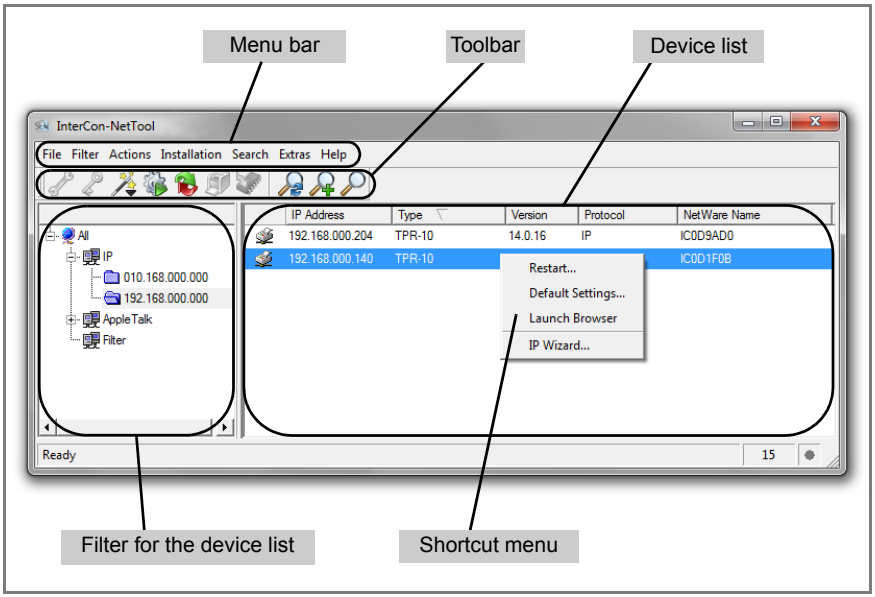


Fig. 2: InterCon-NetTool - Main Dialog

Which Functions Are Supported?

The InterCon-NetTool allows you to

- assign an IPv4 address to the TPR ⇨ 26
- restart the TPR ⇨ 91
- reset the parameter values of the TPR to their default settings ⇨ 87
- start the TPR Control Center ⇨ 18
- switch from the BIOS mode to the default mode ⇨ 120

Detailed information on how to use the InterCon-NetTool can be found in the Online Help. To start the Online Help, select **Help – Online Help** from the menu bar.

2.3 Administration via Email

You can administer the TPR via email and thus via any computer with Internet access.

Functionalities

An email allows you to

- send TPR status information
- specify TPR parameters or
- perform an update on the TPR.

Requirements

☑ In order to receive emails, the TPR must be set up as user with its own email address on a POP3 server.

☑ A DNS server has been configured on the TPR; see: ⇨ 30.

☑ POP3 and SMTP parameters have been configured on the TPR; see: ⇨ 32.

Sending Instructions via Email

If you want to administer the TPR, you must enter the relevant instructions into the subject line of your email.

Proceed as follows:

1. *Open an email program.*
2. *Write a new email.*
3. *Enter the TPR address as recipient.*
4. *Enter an instruction into the subject line; see: 'Syntax and Format of an Instruction'* ⇨ *22*.
5. *Send the email.*

The TPR receives the email and carries out the instruction.

Syntax and Format of an Instruction

Note the following syntax for instructions in the subject line:
`cmd: <command> [<comment>]`

The following commands are supported:

Commands	Option	Description
<command>	get status	Sends the status page of the TPR.
	get parameters	Sends the parameter list of the TPR.
	set parameters	Sends parameters to the TPR. The syntax and values can be obtained from the parameter list, see: ⇨ 100. Parameter and value must be entered into the email body.
	update TPR	Carries out an automatic update using the software that is attached to the email.
	help	Sends a page containing information about the remote maintenance.
[<comment>]		Freely definable text for descriptions.

The following applies for the instructions:

- not case-sensitive
- one or more space characters are allowed
- max. length is 128 byte
- only the ASCII format can be read

Security with TAN

You will need a TAN for updates or parameter changes on the TPR. You will get a current TAN from the TPR via email, e.g. when receiving a status page. Enter the TAN into the first line of the email body. A space character must follow.

Parameter Changes

Parameter changes are integrated into the email body with the following syntax:

<parameter> = <value>

The syntax and values can be obtained from the parameter list, see: ⇨ 100.

Example 1

This email causes the TPR to send the parameter list to the sender of the email.

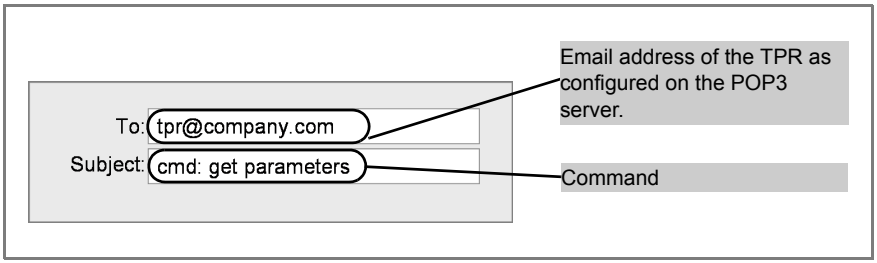


Fig. 3: Administration via Email - Example 1

Example 2

This email configures the parameter 'Description' on the TPR.

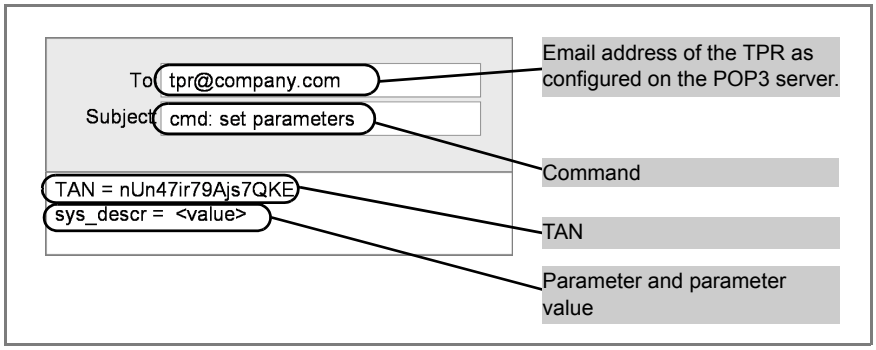


Fig. 4: Administration via Email - Example 2

2.4 Administration via the Status/Reset Button of the Device

LEDs, various ports and the status/reset button can be found on the TPR. These components are described in the 'Quick Installation Guide'.

The status/reset button allows you to

- print a status page; see: ⇨ 92.
- print a service page; see: ⇨ 92.
- reset the TPR parameters to their default settings; see: ⇨ 87.

3 Network Settings

You can define various settings for an ideal integration of the TPR into a network. This chapter describes which network settings are supported.

What information do you need?

- 'How to Configure IPv4 Parameters' ⇨26
- 'How to Configure IPv6 Parameters' ⇨28
- 'How to Configure the DNS' ⇨30
- 'How to Configure SNMP' ⇨31
- 'How to Configure POP3 and SMTP' ⇨32
- 'How to Configure Bonjour' ⇨35
- 'How to Configure the Device Time' ⇨36

3.1 How to Configure IPv4 Parameters

TCP/IP (Transmission Control Protocol over Internet Protocol) forwards data packets across several connections and establishes a connection between the network participants.

The boot protocols DHCP and BOOTP belong to the TCP/IP protocol family. You can define various IPv4 parameters for an ideal integration of your TPR into a TCP/IP network. For further information about the assignment of IP addresses, see: ⇨ 13.

What do you want to do?

☐ 'Configuring IPv4 Parameters via the TPR Control Center' ⇨ 26

☐ 'Configuring IPv4 Parameters via the InterCon-NetTool' ⇨ 27

Configuring IPv4 Parameters via the TPR Control Center

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **NETWORK - IPv4**.
3. *Configure the IPv4 parameters; see: Table 2* ⇨ 26.
4. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Table 2: IPv4Parameters

Parameters	Description
DHCP BOOTP ARP/PING	Enables or disables the protocols DHCP, BOOTP, and ARP/PING. *Protocols offer various possibilities to save the IP address in the TPR.* *(See 'Saving the IP Address in the TPR'* ⇨ 13.*)* We recommend disabling these options once an IP address has been assigned to the TPR.
IP address	IP address of the TPR
Subnet mask	Subnet mask of the TPR
Gateway	Gateway address of the TPR

Configuring IPv4 Parameters via the InterCon-NetTool

Requirements

☑ The InterCon-NetTool is installed on the client, see: ⇨ 20.

☑ The network scan via Multicast has been enabled in the InterCon-NetTool.

☑ The router in the network forwards multicast requests.

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Highlight the TPR in the device list.*
   The TPR-10 is displayed in the device list under 'ZeroConf' with an IP address from the address range (169.254.0.0/16) which is reserved for ZeroConf.
3. *Select* **Installation – IP Wizard** *from the menu bar.*
   The IP Wizard is started.
4. *Follow the instructions of the IP Wizard.*

The settings are saved.

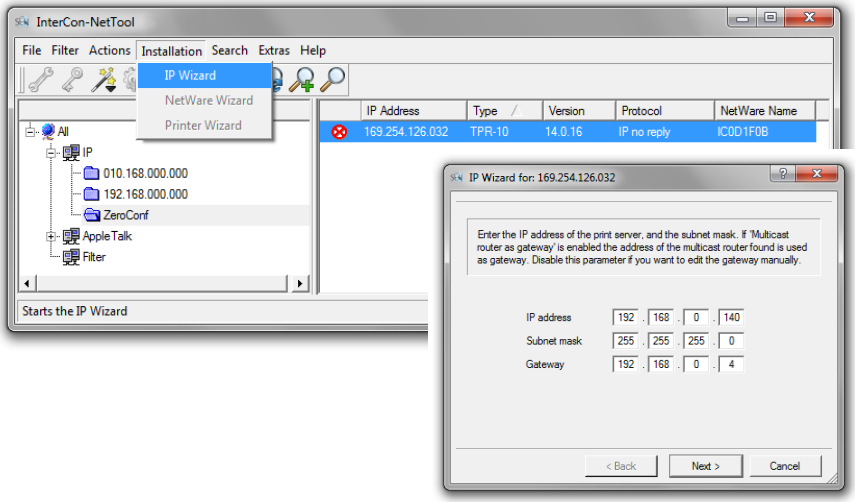

InterCon-NetTool
File Filter Actions Installation Search Extras Help
IP Wizard
NetWare Wizard
Printer Wizard
IP Address Type Version Protocol NetWare Name
169.254.126.032 TPR-10 14.0.16 IP no reply IC0D1F0B
All
IP
010.168.000.000
192.168.000.000
ZeroConf
AppleTalk
Filter
Starts the IP Wizard
IP Wizard for: 169.254.126.032
Enter the IP address of the print server, and the subnet mask. If 'Multicast router as gateway' is enabled the address of the multicast router found is used as gateway. Disable this parameter if you want to edit the gateway manually.
IP address 192 . 168 . 0 . 140
Subnet mask 255 . 255 . 255 . 0
Gateway 192 . 168 . 0 . 4
< Back
Next >
Cancel

Fig. 5: InterCon-NetTool - IP Wizard

3.2 How to Configure IPv6 Parameters

You can integrate the TPR into an IPv6 network.

What are the Advantages of IPv6?

IPv6 (Internet Protocol version 6) is the successor of the more common IPv4. Both protocols are standards for the network layer of the OSI model and regulate the addressing and routing of data packets via a network. The introduction of IPv6 has many benefits:

- IPv6 increases the IP address space from 2^{32} (IPv4) to 2^{128} (IPv6) IP addresses
- Auto Configuration and Renumbering
- Efficiency increase during routing due to reduced header information
- Integrated services such as IPSec, QoS, Multicast
- Mobile IP

What is the Structure of an IPv6 Address?

An IPv6 address consists of 128 bits. The normal format of an IPv6 address is eight fields. Each field contains four hexadecimal digits representing 16 bits.

Each field is separated by a colon (:).
Example: `fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4`

Leading zeros in a field can be omitted.
Example: `fe80 : 0 : 0 : 0 : 0 : 10 : 1000 : 1a4`

An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used. However, the use of two colons can be used only once in an address.
Example: `fe80 : : 10 : 1000 : 1a4`

As a URL in a Web browser, an IPv6 address must be enclosed in brackets. This prevents port numbers from being mistakenly regarded as part of an IPv6 address.
Example: `http://[2001:608:af:1::100]:443`

The URL will only be accepted by browsers that support IPv6.

Which Types of IPv6 Addresses are available?

There are different types of IPv6 addresses. The prefixes of the IPv6 addresses provide information about the IPv6 address types.

- Unicast addresses can be routed globally. These addresses are unique and therefore unambiguous. A packet that is sent to a unicast address will only arrive to the interface that is assigned to this address. Unicast addresses have the prefixes '2' or '3'.
- Anycast addresses are assigned to more than one interface. This means that a data packet that is sent to this address will arrive at various devices. The syntax of anycast addresses is the same as the one of unicast addresses. The difference is that anycast addresses choose one interface out of many.
  A packet that is dedicated to an anycast address arrives at the nearest interface (in line with the router metrics). Anycast addresses are only used by routers.
- Multicast addresses allow you to send data packets to different interfaces at the same time without a proportional increase of the bandwidth. A multicast address can be recognized by the prefix 'ff'.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **NETWORK – IPv6**.
3. *Configure the IPv6 parameters; see: Table 3* ⇨ *30.*
4. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Table 3: IPv6 Parameters

Parameters	Description
IPv6	Enables/disables the IPv6 functionality of the TPR.
Automatic configuration	Enables/disables the automatic assignment of the IPv6 address for the TPR.
IPv6 address	Defines a manually assigned IPv6 Unicast address in the n:n:n:n:n:n:n:n format for the TPR. *Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.*
Router	Defines the IPv6 unicast address of the router. The TPR sends its 'Router Solicitations' (RS) to this router.
Prefix length	Defines the length of the subnet prefix for the IPv6 address. The value 64 is preset. *Address ranges are indicated by prefixes. The prefix length (number of bits used) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/'.*

3.3 How to Configure the DNS

DNS is a service that translates domain names into IP addresses. Using DNS, names can be assigned to IP addresses and vice versa. If a DNS server is available in your network, you can use DNS for your TPR.

If you use a domain name during the configuration process, you must first enable and configure DNS. DNS is used for the configuration of the time server, for example.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **NETWORK – DNS**.
3. *Configure the DNS parameters; see: Table 4* ⇨ 31.
4. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Table 4: DNS Parameters

Parameters	Description
DNS	Enables/disables the name resolution via a DNS server.
Primary DNS server	Specifies the IP address of the primary DNS server (e.g. 192.168.0.21).
Secondary DNS server	Defines the IP address of the secondary DNS server. *The secondary DNS server is used if the first one is not available.*
Domain name (suffix)	Defines the domain name of an existing DNS server (e.g. company.de).

3.4 How to Configure SNMP

SNMP (Simple Network Management Protocol) has become the standard protocol for the administration and monitoring of network elements. The protocol controls communication between the monitored devices and the monitoring station.

SNMP allows you to read and edit management information provided by the network elements (e.g. the TPR or printer). The TPR supports versions 1 and 3 of SNMP.

SNMPv1

The SNMP community is a basic form of access protection. A large number of SNMP managers are grouped together in the community. The community is then assigned (read/write) access rights. The general community string is 'public'.

The community string for SNMPv1 is transferred in plain text and does not provide sufficient protection.

SNMPv3

SNMPv3 is a continuation of the SNMP standard, which provides improved applications and a user-based security model. Distinguishing features of SNMPv3 include its simplicity and security concept.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **NETWORK - SNMP**.
3. *Configure the SNMP parameters; see: Table 5* ⇨ 32.
4. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Table 5: SNMP Parameters

Parameters	Description
SNMPv1	Enables/disables SNMPv1.
Read-only	Enables/disables the write protection for the community.
Community	SNMP community name *The SNMP community is a basic form of access protection in which several participants with the same access rights are grouped together.*
SNMPv3	Enables/disables SNMPv3.
User name	Defines the name of the SNMP user.
Password	Defines the password of the SNMP user.
Hash	Defines the hash algorithm.
Access rights	Defines the access rights of the SNMP user.
Encryption	Defines the encryption method.

3.5 How to Configure POP3 and SMTP

You must configure the protocols POP3 and SMTP on the TPR so that the notification service (⇨ 41) and the administration via email (⇨ 22) will work properly.

POP3

'POP3' (Post Office Protocol Version 3) is a transfer protocol that a client can use to fetch emails from a mail server. POP3 is required in the TPR to administer the TPR via email.

SMTP

'SMTP' (Simple Mail Transfer Protocol) is a protocol that controls the sending of emails in networks. SMTP is required in the TPR to administer the TPR via email and to run the notification service.

What do you want to do?

☐ 'Configuring POP3' ⇨ 33

☐ 'Configuring SMTP' ⇨ 34

Configuring POP3

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **NETWORK - Email**.
3. *Configure the POP3 parameters; see: Table 6* ⇨ *33.*
4. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Table 6: POP3 Parameters

Parameters	Description
POP3	Enables/disables the POP3 functionality.
POP3 - Server name	Name of the POP3 server.
POP3 - Server port	Defines the port used by the TPR for receiving emails. The port number 110 is preset. When using SSL/TLS, enter 995 as port number.
POP3 - Security	Defines the authentication method to be used (APOP / SSL/TLS). When using SSL/TLS, the cipher strength is defined via the encryption level ⇨ 61.
POP3 - Check mail every	Defines the time interval (in minutes) for retrieving emails from the POP3 server.
POP3 - Ignore mail exceeding	Defines the maximum email size (in Kbyte) to be accepted by the TPR. *(0 = unlimited)*
POP3 - User name	Defines the user name used by the TPR to connect to the POP3 server.
POP3 - Password	Defines the user password used by the TPR to connect to the POP3 server.

Configuring SMTP

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **NETWORK - Email**.
3. *Configure the SMTP parameters; see: Table 7* ⇨ 34.
4. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

Table 7: SMTP Parameters

Parameters	Description
SMTP - Server name	Defines the name of the SMTP server.
SMTP - Server port	Defines the port number used by the TPR to send emails to the SMTP server. The port number 25 is preset.
SMTP - TLS	Enables/disables TLS. *The security protocol TLS (Transport Layer Security) is used to encrypt the transmission between the TPR and the SMTP server. The cipher strength is defined via the encryption level* ⇨ 61.
SMTP - Sender name	Defines the email sender name to be used by the TPR.
SMTP - Login	Enables/disables the SMTP authentication for the login.
SMTP - User name	Defines the user name for the SMTP authentication.
SMTP - Password	Defines the password for the SMTP authentication.
SMTP - Security (S/MIME)	Enables/disables the encryption and signing of emails via S/MIME.
SMTP - Signing emails	Defines the signing of emails. *A signature created by the sender allows the recipient to verify the identity of the sender and to make sure that the email was not modified. An S/MIME certificate (*⇨ 67) *is required for the signing of emails.*
SMTP - Full encryption	Defines the encryption of emails. *Only the recipient can open and read the encrypted email. An S/MIME certificate (*⇨ 67) *is required for the encryption.*

Parameters	Description
SMTP- Attach public key	Sends the public key together with the email. Many email clients require the public key to be attached in order to view the emails.

3.6 How to Configure Bonjour

Bonjour allows the automatic recognition of computers, devices, and network services in TCP/IP-based networks.

The TPR uses the following Bonjour functions:

- Checking the IP address assigned via ZeroConf
- Assignment of host names to IP addresses
- Location of server services without knowledge of the device's host name or IP address.

When checking the IP address assigned via ZeroConf (see: 'ZeroConf' ⇨14) the TPR sends a query to the network. If the IP address has already been assigned elsewhere in the network, the TPR will receive a message. The TPR then sends another query with a different IP address. If the IP address is available, it is saved in the TPR.

The domain name service is used for additional Bonjour features. Since there is no central DNS server in Bonjour networks, each device and application has its own small DNS server.

This integrated DNS server (mDNS) collects and administers the information of all participants in the net. In addition to the features of a classical DNS server, the mDNS server also saves the IP address, the service name and the offered services of each participant.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **NETWORK - Bonjour**.
3. *Configure the Bonjour parameters; see: Table 8* ⇨36.
4. *Click* **Save & Restart** *to confirm.*

The setting will be saved.

Table 8: Bonjour Parameters

Parameters	Description
Bonjour	Enables/disables Bonjour.
Bonjour name	Defines the Bonjour name of the TPR. *The TPR uses this name for its Bonjour services. If no Bonjour name is entered, the default name will be used (device name@ICxxxxxx).*

3.7 How to Configure the Device Time

You can set the time of the TPR via a time server (SNTP server) in the network. A timeserver is a computer networking device that reads the actual time from a reference clock and distributes this information to its clients. In the TPR, the time server is defined via the IP address or the host name.

Benefits and Purpose

If the time server is activated, the ThinPrint print jobs that are handled by the TPR will get a time stamp. Date and time are then displayed under (⇨94) 'Job History'.

UTC

The TPR uses 'UTC' (Universal Time Coordinated) as a basis. UTC is a reference time and used as a time standard.

Time zone

The time received by the time server does not necessarily correspond to your local time zone. Deviations from your location and the resulting time difference (including country-specific particularities such as Daylight Saving Time) can be handled by means of the 'Time zone' parameter.

Requirements

☑ A time server is integrated into the network.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **NETWORK - Date/Time**.
3. *Tick* **Date/Time**.

4. *Enter the IP address or the host name of the time server into the* **Time server** *box.*
   (A host name can only be used if a DNS server was configured beforehand.)
5. *Select the code for your local time zone from the* **Time zone** *list.*
6. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

4 Device Settings

The TPR allows you to configure descriptions, communication with the printer, local service ports and the notification service. This chapter describes these device settings.

What information do you need?

- 'How to Determine a Description' ⇨ 38
- 'How to Configure the Communication between the TPR and the Printer' ⇨ 38
- 'How to Define Local Service Ports' ⇨ 40
- 'How to Use the Notification Service' ⇨ 41

4.1 How to Determine a Description

You can assign freely definable descriptions to the TPR. This gives you a better overview of the devices available in the network.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE – Description**.
3. *Enter freely definable names for* **Host name, Description** *and* **Contact person**.
4. *Click* **Save & Restart** *to confirm.*

The data is saved.

4.2 How to Configure the Communication between the TPR and the Printer

Internal IP Network

The TPR must be physically connected to the printer and the network. Both devices build an internal local network in which the TPR has a second, local IP address for the internal communication

with the printer. The internal DHCP server of the TPR automatically configures the IP address of the printer and the related parameters.

Masquerading (NAT)

In order to connect the internal network to the external network, the address information is rewritten via masquerading. Masquerading is a type of NAT (Network Address Translation). This way, data packets are forwarded by the TPR to the printer. The TPR is integrated in a transparent way and the infrastructure as well as (possibly) existing output monitoring systems remain unaffected.

You can adjust the settings of the internal network.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE - TPR-10**.
3. *Configure the printer parameters; see: Table 9* ⇨ 39.
4. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Table 9: Printer Configuration

Parameters	Description
Local IP address	Defines the IP address of the TPR for the internal communication. *The TPR and printer constitute an internal IP network. The local IP address is the gateway to the printer IP address. The subnet mask is 255.255.255.240.*
Printer IP address	Defines the IP address of the printer for the internal communication. *The TPR and printer constitute an internal IP network. The printer IP address and related parameters are set by the internal DHCP server of the TPR.*
Masquerading	Enables/disables masquerading. *Masquerading is a type of NAT (Network Address Translation). In NAT, all external IP addresses are translated to the local IP address.*
ICMP	Enables/disables the routing of ICMP packets to the printer IP address. *In IP networks, ICMP is used to transmit error messages and queries, for example 'ping'. If the option is enabled, queries will be answered by the printer and not by the TPR.*

4.3 How to Define Local Service Ports

The TPR utilizes TCP ports for the data transfer in the network. TCP ports are address components that are characterized by their port number. Ports are used to establish connections and to assign data packets to the correct services.

Certain services (HTTP, HTTPS, SNMP, etc.) have permanently assigned ports.

You can specify port numbers for the following local services:

- HTTP (Default = 80)
- HTTPS (Default = 443)
- SNMP (Default = 161)
- ThinPrint (Default = 4000)

TCP ports that are configured as local service ports cannot be used for the communication with the printer. Assign free port numbers to the local service ports in order to use the default TCP ports for the communication with the printer.

Example

If you assign the port number 8080 to HTTP, the printer homepage is displayed when entering the IP address of the TPR into the browser. To open the TPR Control Center, add the port number to the IP address (<IP address>:8080). In the InterCon-NetTool, the TPR appears as printer ('Type' column).

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE - TPR-10**.
3. *Enter the port numbers into the relevant boxes in the* **Local services ports** *area.*
4. *Click* **Save & Restart** *to confirm.*

The settings are saved.

4.4 How to Use the Notification Service

You can get notifications in the form of emails or SNMP traps from the TPR. By means of these notifications up to four email recipients can be informed about various events irrespective of time and location.

The following message types are possible:

- The status email periodically informs the recipient about the status of the TPR.
- The event notification informs you about a specific event on the TPR via email or SNMP trap. The event can be:
  - The restart of the TPR.
  - A card event on the TPR.
  - The connection or disconnection of a USB flash drive to/from the TPR.
  - A problem with the TPR.

What do you want to do?

- ☐ 'Configuring the sending of status emails' ⇨📄41
- ☐ 'Configuring event notifications via email' ⇨📄42
- ☐ 'Configuring event notifications via SNMP traps' ⇨📄42

Configuring the sending of status emails

Requirements

- ☑ SMTP parameters can be configured on the TPR, see: ⇨📄32.
- ☑ A DNS server has been configured on the TPR; see: ⇨📄30.

For the notification service you can specify up to two email recipients.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE - Notification**.
3. *Enter the email address of the recipient into the* **Email recipient** *box.*
4. *Tick* **Status** *for the relevant recipient.*

5. *Specify the sending interval in the* **Status notification time** *area.*
6. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

Configuring event notifications via email

Requirements

☑ SMTP parameters can be configured on the TPR, see: ⇨ 32.

☑ A DNS server has been configured on the TPR; see: ⇨ 30.

For the notification service you can specify up to two email recipients and the message types.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE - Notification**.
3. *Enter the email address of the recipient into the* **Email recipient** *box.*
4. *Tick the options with the desired message types.*
5. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

Configuring event notifications via SNMP traps

For the notification service you can specify up to two SNMP trap recipients and the message types.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE - Notification**.
3. *Enter the trap address of the recipient into the* **Trap target** *box.*
4. *Enter the trap community of the recipient into the* **Trap community** *box.*
5. *Tick the options with the desired message types.*
6. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

5 Personal Printing Settings

You must define server and printer settings so that the TPR is able to communicate with the Personal Printing server, carry out the authentication process and receive and forward print jobs. This chapter describes how to match the parameter values in an ideal way.

What information do you need?

- 'How to Define the Personal Printing Server' ⇨📄44
- 'How to Encrypt the Connection to the Personal Printing Server' ⇨📄45
- 'How to Verify the Identity of the Personal Printing Server' ⇨📄46
- 'How to Configure the Personal Printing Printer' ⇨📄47

The settings described here refer to the client-side (TPR). Information about the installation, configuration and administration of the Personal Printing environment can be found in the Personal Printing documentation at http://www.thinprint.com.

5.1 How to Define the Personal Printing Server

In Personal Printing environments, print jobs are buffered on the Personal Printing server. The print jobs will be forwarded and printed once the user has successfully authenticated to the TPR.

Connection

You must define the server name and port so that a connection to the Personal Printing server can be established.

Authentication Process

You need a User-PIN for the authentication process on the Personal Printing server. You do not need to enter an individual PIN because the authentication to the TPR is done via a chip card. All users of the TPR will get the same user-PIN. This PIN will be defined on the Personal Printing server and must be saved identically to the TPR.

Configure a default user-PIN (e.g. 'SEH') on the Personal Printing server for all users of the TPR. The user-PIN 'SEH' is preset on the TPR.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE - Personal Printing**.
3. *Tick* **Personal Printing**.
4. *Specify the Personal Printing parameters; see: Table 10* ⇨ 44.
5. *Click* **Save & Restart** *to confirm.*

The setting will be saved.

Table 10: Personal Printing Parameters

Parameters	Description
Server name	Defines a Personal Printing server via the IP address or the host name. *The host name can only be used if a DNS server was configured beforehand.*
Server port	Defines the TCP port used by the TPR for communicating with the Personal Printing server. *The port number 80 is preset. When using SSL, enter 443 as port number (⇨ 45).*

Parameters	Description
User-PIN	Defines the User-PIN. *The specified User-PIN and the User-PIN in the user accounts of the Active Directory must be identical. The preset user-PIN is 'SEH'.*

5.2 How to Encrypt the Connection to the Personal Printing Server

A secure connection between the Personal Printing server and the TPR can be achieved by using an SSL/TLS encryption. When querying print jobs, the user data (user-ID, user-PIN, etc.) will be transmitted in an encrypted way. The cipher strength is defined via the encryption level ⇨61.

In this process, the Personal Printing protocol, which establishes the connection between the Personal Printing server and the TPR and transmits the data packets, will be encrypted via SSL/TLS. This means that certificates are needed for the authentication.

A certificate from a matching CA (Certification Authority) must be installed both on the Personal Printing server and the TPR.

The Personal Printing server requests a CA certificate from the TPR. By means of the related root certificate, the CA certificate will be verified by the Personal Printing server. To this purpose, the root certificate must be stored on the Personal Printing server.

Procedure

- Create a certificate request on the TPR; see: 'Creating a Certificate Request for CA Certificates' ⇨71.
- Create a CA certificate using the certificate request and the certification authority.
- Install the CA certificate on the TPR; see: 'Saving the CA Certificate on the TPR' ⇨72.
- Install the root certificate of the certification authority on the Personal Printing server.
- Enable the SSL/TLS encryption on the TPR.

Requirements

☑ The port number of the Personal Printing server is set to 443; see: ⇨📄44.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE - Personal Printing**.
3. *Tick* **SSL connection**.
4. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

5.3 How to Verify the Identity of the Personal Printing Server

The identity of the Personal Printing server can be verified by means of certificates. If the verification fails, no connection to the Personal Printing server will be established.

If the verification of the identity was enabled for Personal Printing, a certificate from a matching CA (Certification Authority) must be installed both on the Personal Printing server and the TPR.

The TPR requests a Personal Printing certificate (server certificate) from the Personal Printing server. By means of the related root certificate and/or Personal Printing certificate, the TPR verifies the certificate (and thus its identity) of the Personal Printing server.

Requirements

☑ A Personal Printing certificate is saved on the Personal Printing server.

☑ A root certificate and/or Personal Printing certificate is saved on the TPR (⇨📄67).

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE - Personal Printing**.
3. *Tick* **Verify certificate**.
4. *Click* **Save & Restart** *to confirm.*

↳ The setting will be saved.

5.4 How to Configure the Personal Printing Printer

The authentication for retrieving print jobs is done directly on the TPR, i.e. on the printer.

Before you can use a printer for Personal Printing, you must first set up the printer on the Personal Printing server. It will automatically get a printer ID. The print jobs are assigned via the printer ID.

The printer that is connected to the TPR must then be integrated to the TPR. To this purpose, you must define the printer ID on the TPR. The printer ID must be identical to the ID on the Personal Printing server.

You can configure various parameters to customize the print output.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE - Personal Printing**.
3. *Enter the ID of the connected printer into the* **Printer ID** *box.*
4. *Specify the parameters for the print output; see: Table 11* ⇨ *47.*
5. *Click* **Save & Restart** *to confirm.*

The setting will be saved.

Table 11: Print Output Parameters

Parameters	Description
Trigger print jobs separately	Enables/disables the release of one single print job per cardswipe. If several print jobs are available, they have to be released individually one after another.
Job deletion by server	Enables/disables the immediate deletion of printed jobs by the Personal Printing server. *This setting will override any settings for the deletion of printed jobs set on the Personal Printing server. If neither the job deletion by server nor the job deletion by TPR is enabled, printed jobs will be deleted as defined in the settings on the Personal Printing server.*

Parameters	Description
Job deletion by TPR	Enables/disables the deletion of printed jobs by the TPR. The time of deletion can be defined via the delay. *This setting will override any settings for the deletion of printed jobs set on the Personal Printing server. If neither the job deletion by server nor the job deletion by TPR is enabled, printed jobs will be deleted as defined in the settings on the Personal Printing server.*
Delay	Defines a delay (in seconds) for the deletion of printed jobs by the TPR. (0 = immediate deletion) *A delay assures the complete transfer to the printer and printout of the print job.*
Beeper	Enables/disables the audio feedback. Acoustic signals give information about the triggering of print jobs; see 'Quick Installation Guide'.

6 ThinPrint Settings

The TPR can additionally be used as ThinPrint gateway. You must define the port, the bandwidth as well as the printer and the printer properties if you want the TPR to communicate with a ThinPrint server via a port or if you want the TPR to receive and forward print jobs. This chapter describes how to match the parameter values in an ideal way.

What information do you need?

- 'How to Define the ThinPrint Port' ⇨ 50
- 'How to Define the Bandwidth' ⇨ 50
- 'How to Embed the Printer' ⇨ 51
- 'How to Define Timeouts' ⇨ 53
- 'How to Get Status Information on the Printer Connection' ⇨ 54
- 'How to Get Printer Messages' ⇨ 56
- 'How to Use the ThinPrint Connection Service' ⇨ 57
- 'How Does the TPR Receive Encrypted Data?' ⇨ 59

The settings described here refer to the client-side (TPR). Information about the installation, configuration and administration of the ThinPrint environment can be found in the ThinPrint documentation at http://www.thinprint.com.

6.1 How to Define the ThinPrint Port

In ThinPrint environments, printing is done to a TCP/IP port via a socket connection. The port number of the TPR must be identical to the port number that was defined for the ThinPrint server.

Port 4000 is preset on the TPR. You can change the port number, if necessary.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE – ThinPrint®**.
3. *Enter the port number into the* **ThinPrint® port** *box.*
4. *Click* **Save & Restart** *to confirm.*

The setting will be saved.

6.2 How to Define the Bandwidth

Bandwidth describes the capacity of a data connection. The bandwidth of the TPR is indicated in bit/second (bit/s).

The bandwidth that is needed for print jobs can be limited to a freely definable value for each ThinPrint port (server side). You can further decrease the bandwidth limit on the port of the TPR (client side).

Defining a bandwidth value on the TPR which is higher than the defined value (server side) will have no effect. In this case, the pre-defined value will be applied.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE – ThinPrint®**.
3. *Tick* **Bandwidth**.
4. *Enter the desired bandwidth.*
5. *Click* **Save & Restart** *to confirm.*

The setting will be saved.

6.3 How to Embed the Printer

Print jobs are sent from the ThinPrint server to the TPR. After the decompression of the print jobs, the TPR forwards the print jobs to the printers.

The print jobs are assigned via the printer ID. A network printer can be integrated via the TPR.

When integrating the connected network printer, you must define the printer parameters (name, class, driver) and a transfer method.

Transfer Methods

The data transfer between the TPR and the network printer can be done in three ways:

- Usually the data is transferred to the TCP/IP port via a **raw/socket connection**. Port 9100 is preset on the TPR. If required, you can configure a different port number.
- By means of **IPP connections** (Internet Printing Protocol) the print data is transmitted via HTTP 1.1 via local networks or the Internet to the printer. To this purpose, you must configure a printer URL that needs to be implemented according to the information of the manufacturer. Please refer to the documentation of your printer. The printer URL 'ipp/lp1' is preset and can be changed, if needed.
  Your advantage: The connection between the TPR and the printer can be encrypted via SSL/TLS.
- Data transfer can also be done via the **LPD protocol** (Line Printer Daemon). During LPD printing the print data is sent to the IP address of the printer by means of an LPD queue.
  The LPD queue name 'lp1' is preset. If required, you can configure a different LPD queue name. Depending on the configuration, the printing behavior is either compliant to RFC1179 or resembles Microsoft LPD printing.
  Your advantage: When using the LPD protocol for data transfer, additional print job attributes will be transferred and displayed in the 'job history' (⇨ 94).

The support of the transfer methods depends on the printer. Consult your printer manual for more information.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE – ThinPrint®**.
3. *Enter the printer parameters into the boxes; see: Table 12* ⇨ *52.*
4. *Select a transfer method for the printer.*
5. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Table 12: Printer Parameters

Parameters	Description
ID	The ID clearly identifies the printer for the ThinPrint server.
Printer	Defines the printer name. The printer name is purely a description and is used to distinguish the printers. *The printer can only use the ThinPrint AutoConnect feature if a printer name was defined. If the printer supports SNMP, the printer class is derived automatically via SNMP. A freely definable description can be entered at any time and will override any automatically derived printer name.*
Class	Printers with compatible drivers can be arranged in one class. *In addition to the defining of the printer name, you can also define a printer class if you want to use the ThinPrint AutoConnect feature. If the printer supports SNMP, the class name is obtained automatically via SNMP. A freely definable description can be entered at any time and will override any automatically derived class name.*
Driver	Defines the printer driver for the ThinPrint® AutoConnect feature.
Port	Defines the port number for RAW/socket printing. (Default = 9100) *Is used when selecting 'RAW' as the transfer method.*

Parameters	Description
URL	Specifies the second part of the printer URL for IPP printing. (Default = ipp/lp1) *Is used when selecting 'IPP' as the transfer method.*
SSL	Enables/disables the SSL/TLS encryption for IPP printing. The cipher strength is defined via the encryption level ⇨ 61. *Is used when selecting 'IPP' as the transfer method.*
LPD Queue	Defines the queue name for LPD printing. (Default = lp1) *Is used when selecting 'LPD' as the transfer method.*
RFC	Enables/disables the RFC1179 conformity for LPD printing. *Is used when selecting 'LPD' as the transfer method. If this option is disabled, the printing behavior resembles that of Microsoft® LPD printing.*

6.4 How to Define Timeouts

You can use timeouts to control how errors are handled before and during a print job.

Printer connection timeout

The 'Printer open timeout' parameter specifies the period of time (in seconds) after which a connection attempt to the printer should be aborted. It is advisable to abort a connection attempt if the printer is not physically available for the TPR and the ThinPrint port is to be freed for subsequent print jobs, for example.

Job sending timeout

The 'Job send timeout' parameter specifies the period of time (in seconds) after which a current print job should be aborted. It is advisable to abort a print job if the print job cannot be executed due to a printer error (for example, no paper).

Both timeouts cause the print jobs to be deleted. In 'pure' ThinPrint printing, an error message is also sent to the ThinPrint server. No error message is sent to the ThinPrint server when printing takes place via the Connection Service.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE – ThinPrint®**.
3. *In the* **Printer connection timeout** *and* **Job sending timeout** *fields, enter the periods of time in seconds after which the timeouts should take effect (0 s = off).*
4. *Click* **Save & Restart** *to confirm.*

The settings are saved.

6.5 How to Get Status Information on the Printer Connection

You can view the connection statuses of the embedded printer. The following connection statuses can be displayed:

Connection Status	Description
Time out	No connection to the printer at present. A connection was available at an earlier stage.
reachable	A connection to the printer is available at present.
unreachable	No connection to the printer so far.
Unknown	The connection status to the printer cannot be determined.

In order to get the connection status, you must configure a 'ping' query.

What do you want to do?

- ☐ 'Configuring a 'ping' Query via the TPR Control Center' ⇨ 55
- ☐ 'Displaying the Printer Connection Status via the TPR Control Center' ⇨ 55

Configuring a 'ping' Query via the TPR Control Center

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE – ThinPrint® printer.**
3. *Tick* **Monitoring via ping**.
4. *Enter the interval (in seconds) into the* **Monitoring interval** *box.*
5. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Displaying the Printer Connection Status via the TPR Control Center

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE – ThinPrint® printer.**

The printer connection status is displayed under 'ThinPrint® printer status' in the 'Status' row.

6.6 How to Get Printer Messages

You can view printer error messages (Paper empty, Offline, Paper jam, etc.) and printer status messages (idle, printing, warming up, etc.).

In order to get printer messages, you must configure an SNMP query beforehand. Not all printers support SNMP. Consult your printer manual for more information.

What do you want to do?

- ☐ 'Configuring an SNMP Query via the TPR Control Center' ⇨📄56
- ☐ 'Displaying Printer Status Messages via the TPR Control Center' ⇨📄56

Configuring an SNMP Query via the TPR Control Center

Requirements

☑ The printer supports SNMP.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE – ThinPrint® printer.**
3. *Tick* **SNMP.**
4. *Enter the interval (in seconds) into the* **Monitoring interval** *box.*
5. *Click* **Save & Restart** *to confirm.*

↳ The settings are saved.

Displaying Printer Status Messages via the TPR Control Center

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE – ThinPrint® printer.**

↳ The printer messages will be displayed under 'ThinPrint® printer status' in the 'Status' row.

6.7 How to Use the ThinPrint Connection Service

The ThinPrint Connection Service sends print jobs via TCP/IP to ThinPrint clients (i.e. the TPR) in masked networks (NAT).

The Connection Service manages the entire communication between the ThinPrint server and the corresponding client. This allows the connection via masked networks as well as the assignment of the relevant print job to the respective end device.

To use this service, you must prepare the TPR. For each end device that uses the Connection Service, you must store the client ID and an authentication key in the database of the Connection Service. You must also set these two values on the TPR.

Please note that you need a ThinPrint license for each client ID.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE – ThinPrint®**.
3. *Tick* **Connection Service**.
4. *Enter the relevant parameters; see: Table 13* ⇨ 57.
5. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Table 13: Connection Service Parameters

Parameters	Description
Connection Service	Enables/disables the ThinPrint Connection Service.
Server name	IP address or host name of the server on which the Connection Service is installed. *The host name can only be used if a DNS server was configured beforehand.*
Port	Defines the TCP port used by the TPR for communicating with the Connection Service. *The port number 4001 is preset.*

Parameters	Description
Client ID	Client ID as stored in the database of the Connection Service. The Connection Service needs the Client ID to send print jobs to the TPR.
Authentication key	Authentication key as stored in the database of the Connection Service.
Keep alive	Interval (in seconds) after which the connection to the Connection Service is refreshed. The value has to be equal to or lower than the 'KeepAliveTO' value set on the Connection Service server. *(allowed entry: 1- 60000 | default = 60)*
Connection retry	Defines the time interval (in seconds) after which a connection retry is executed if the Connection Service cannot be reached. *(allowed entry: 1 - 60000 | default = 120)*

The connection status is displayed in the table 'ThinPrint® status'. If the connection to the Connection Service was refused, it is because a value (client ID, authentication key, port or server name) was entered incorrectly. In this case, verify and correct your settings and click **Save & Restart**.

6.8 How Does the TPR Receive Encrypted Data?

A secure connection during the transfer of print jobs between ThinPrint (server or Connection Service) and the TPR is guaranteed by means of an SSL/TLS encryption. The cipher strength is defined via the encryption level ⇨ 61.

The ThinPrint server requests a certificate from the TPR. By means of this certificate, the ThinPrint server checks whether the TPR is authorized to receive the print data.

If an encryption was enabled on the ThinPrint server, you must install a certificate from a corresponding Certification Authority both on the ThinPrint server and the TPR. To authorize the TPR to receive encrypted print data, proceed as follows:

- Create a certificate request; see: ⇨ 71.
- Save the CA certificate; see: ⇨ 72.

7 Security

A number of security mechanisms are available to ensure optimum security for the TPR. This chapter describes how to make use of these security mechanisms.

What information do you need?

The following security mechanisms can be configured and activated according to your demands:

- 'How to Define the Encryption Level for SSL/TLS Connections' ⇨ 61
- 'How to Control the Access to the TPR Control Center' ⇨ 63
- 'How to Block Individual Ports' ⇨ 64
- 'How to Control the Access to the TPR (TCP Port Access Control)' ⇨ 66
- 'How to Use Certificates Correctly' ⇨ 67
- 'How to Use Authentication Methods' ⇨ 76
- 'How to Configure a Device Assignment' ⇨ 82

7.1 How to Define the Encryption Level for SSL/TLS Connections

The following connections on the TPR can be encrypted via SSL/TLS:

- Email: POP3 (⇨ 32)
- Email: SMTP (⇨ 32)
- Personal Printing: connection to the server (⇨ 44)
- ThinPrint printer: IPP connection (⇨ 51)
- ThinPrint: data encryption (⇨ 45)
- Web access to the TPR Control Center: HTTPS (⇨ 63)

Encryption Level

The encryption strength and thus the safety of the connection is defined via the encryption level.

Cipher Suite

Each encryption level is a collection of so-called cipher suites. A cipher suite is a standardized sequence of four cryptographic algorithms that are used to establish a secure connection. Depending on their cipher strength (in bit), cipher suites are grouped to form an encryption level. Which cipher suites are supported by the TPR, i.e. are part of an encryption level, depends on the protocol used (SSLv2, SSLv3, TLSv1).

Establishing Connections

When establishing a secure connection, a list of supported cipher suites is sent to the communicating party. A cipher suite is agreed upon that will be used later on. The strongest cipher suite that is supported by both parties will be used by default. If there is no cipher suite that is supported by both parties, no SSL/TLS connection will be established.

The communicating parties of the TPR (e.g. browser) must support the cipher suites of the selected encryption level in order to successfully establish a connection. When problems occur, select a different level or reset the parameters of the TPR; see: ⇨ 87.

The following encryption levels can be selected:

- **Compatible:** Cipher suites with an encryption of 40 to 256 bit will be used.
- **Low:** Only cipher suites with a low encryption of 56 bit will be used. (Fast connection)
- **Medium:** Only cipher suites with an encryption of 128 bit will be used.
- **High:** Only cipher suites with a strong encryption of 128 to 256 bit will be used. (Slow connection)

Proceed as follows:

1. *Start the myUTN Control Center.*
2. *Select* **SECURITY – SSL connections**.
3. *Select the desired encryption level from the* **Encryption** *area.*
4. *Click* **Save & Restart** *to confirm.*
5. The setting will be saved.

Detailed information about the individual SSL connection status (e.g. cipher suites) can be found on the Details page at **SSL connection status - Details**.

7.2 How to Control the Access to the TPR Control Center

You are able to restrict the administrative web access to the TPR Control Center with a password or by selecting the permitted types of connection.

What do you want to do?

- ☐ 'Specifying the Permitted Web Connection Type' ⇨📄63
- ☐ 'Protecting the web access via a password' ⇨📄64

The TPR Control Center can also be protected by the SNMP security concept. The concept includes administration of user groups and access rights. For further information; see: 'How to Configure SNMP' ⇨📄31.

Specifying the Permitted Web Connection Type

Types of Connection (HTTP/HTTPS)

The web access to the TPR Control Center can be secured by selecting the permitted types of connection (HTTP/HTTPS).

If HTTPS is exclusively chosen as the connection type, the administrative web access to the TPR Control Center is protected by SSL/TLS. The cipher strength is defined via the encryption level ⇨📄61.

SSL/TLS requires a certificate to check the identity of the TPR. During a so-called 'handshake', the client asks for a certificate via a browser. This certificate must be accepted by the browser. URLs that require an SSL/TLS connection start with 'https'.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY - Device access**.
3. *Tick* **HTTP/HTTPS** *or* **HTTPS only** *in the* **Web** *area.*
4. *Click* **Save & Restart** *to confirm.*

The setting will be saved.

Protecting the web access via a password

You can use a password to protect the TPR Control Center against unauthorized web access. If a password is set, only the start page of the TPR Control Center can be visited and displayed. If you select a menu item, you will be asked to enter a password.

You will also be asked to enter a non-definable user name. Leave this field blank at the password prompt.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY - Device access**.
3. *In the* **web** *area, enter a password into the* **Password** *box.*
4. *Repeat the password.*
5. *Click* **Save & Restart** *to confirm.*

The setting will be saved.

7.3 How to Block Individual Ports

The TPR cannot be attacked directly by viruses. Attacks to open ports can have a certain influence on the TPR and affect its functions.

In order to prevent attacks to open ports, you can block individual ports on the TPR. You can configure, for example, short-term blockings for current security problems (worms, etc.) or long-term blockings of common ports for malware attacks.

Services (e.g. printing via IPP/port 632) can also be blocked by blocking their ports.

Local service ports (⇨ 40) cannot be blocked.

Proceed as follows:

1. *Select* **SECURITY – Port blocking**.
2. *Enter the port number of the port to be blocked into the* **Port** *box.*

3. *Enable the options for the blocking of the desired log types and interfaces.*
   (Both log types and interfaces can be blocked at the same time.)
4. *Click* **Save & Restart** *to confirm.*

↳ The setting will be saved.

To block all TCP or IP ports, see: 'How to Control the Access to the TPR (TCP Port Access Control)' ⇨66.

7.4 How to Control the Access to the TPR (TCP Port Access Control)

TCP Port Access Control

You can control the access to the TPR. To do so, various TCP port types on the TPR can be blocked. Network elements with access rights can be defined as exceptions and excluded from blocking. The TPR only accepts data packets from network elements defined as exceptions.

Security Levels

The port types to be blocked must be defined in the 'Security level' area. The following categorization can be selected:

- Lock TCP access (locks TCP ports: HTTP/HTTPS/...)
- Lock all (locks IP ports)

Exceptions

In order to exclude network elements (e.g. clients, DNS server, SNTP server) from port locking, they must be defined as exceptions. To do so, the IP addresses or MAC addresses (hardware addresses) of the network elements with access rights must be entered in the 'Exceptions' area. Please note:

- MAC addresses are not delivered through routers!
- The use of wildcards (*) allows you to define subnetworks.

Test Mode

The 'test mode' allows you to check the configured access protection. If the test mode is activated, access protection remains active until the TPR is rebooted. After restarting, the protection is no longer effective.

The 'test mode' option is activated by default. After a successful test, you must deactivate the test mode so that access protection remains permanently active.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY - TCP port access**.
3. *Tick* **Port access control**.
4. *Select the desired protection in the* **Security level** *area.*
5. *In the* **Exceptions** *area, define the network elements which are excluded from port blocking. Enter the IP or MAC addresses and tick the options.*
6. *Make sure that the* **test mode** *is enabled.*
7. *Click* **Save & Restart** *to confirm.*
   The settings are saved.
   The port access control is activated until the device is restarted.
8. *Check the port access and configurability of the TPR.*

If the TPR can no longer be reached using the TPR Control Center, restart the device; see: ⇨ 91.

9. *Clear* **Test mode**.
10. *Click* **Save & Restart** *to confirm.*

The settings are saved. The port access control is active. Access to the ports is restricted.

7.5 How to Use Certificates Correctly

The TPR has its own certificate management. This section explains how certificates are used and when the use of certificates is recommended.

What are Certificates?

Certificates can be used in TCP/IP-based networks to encrypt data and to authenticate communication partners. Certificates are electronic messages containing a key (public key) and a signature.

Benefits and Purpose

The use of certificates allows for various security mechanisms. Use certificates in the TPR

- to encrypt the connection to the Personal Printing server; see: ⇨ 45.
- to check the identity of the Personal Printing server; see: ⇨ 46.
- to receive encrypted print data; see: ⇨ 59.
- to check the identity of the TPR in the network; see: 'Configuring EAP-TLS' ⇨ 77.
- to authenticate the TPR/client if the administrative web access to the TPR Control Center is protected via HTTPS (SSL/TLS); see: ⇨ 63.

If you want to use certificates, it is advisable to protect the administrative web access to the TPR Control Center by a password so that the certificate on the TPR cannot be deleted by unauthorized persons; see: ⇨ 63.

Which Certificates are available?

Both self-signed certificates and CA certificates can be used with the TPR. The following certificates can be distinguished:

- **Self-signed certificates** have a digital signature that has been created by the TPR. If a self-signed certificate is used, the ThinPrint server cannot print via SSL/TLS. The connection to the Personal Printing server and the verification of its identity are not possible. A CA certificate is mandatory to print via SSL.
- **CA certificates** are certificates that have been signed by a certification authority (CA).
- The authenticity of the CA certificate can be verified by means of a so-called **root certificate** issued by the certification authority. The root certificate is stored on an authentication server in the network.
- Upon delivery, a certificate (the so-called **default certificate)** is stored in the TPR. It is recommended that you replace the default certificate by a self-signed certificate or CA certificate as soon as possible.

- **S/MIME certificate**
  S/MIME certificates (*.pem file) are used to sign and encrypt the emails that are sent by the TPR. The corresponding private key must be installed as an own certificate in the pkcs(12) format (as *.p12 file) in the intended email program (Thunderbird, Outlook, etc.). Only then can the emails be verified and displayed (in the case of encryption).
- **Personal Printing certificates** are used to verify the identity of the Personal Printing server.

The following certificates can be installed at the same time in the TPR:

- 1 Self-signed certificate

- 1 CA certificate or pkcs(12) certificate

- 1 Root certificate

- 1 S/MIME certificate

- 1 Personal Printing certificate

You can also generate a certificate request for a CA certificate. All certificates can be deleted separately. Existing certificates will be overridden when installing or generating new certificates.

A pkcs(12) certificate can only be installed if there are currently no certificate requests or CA certificates installed.

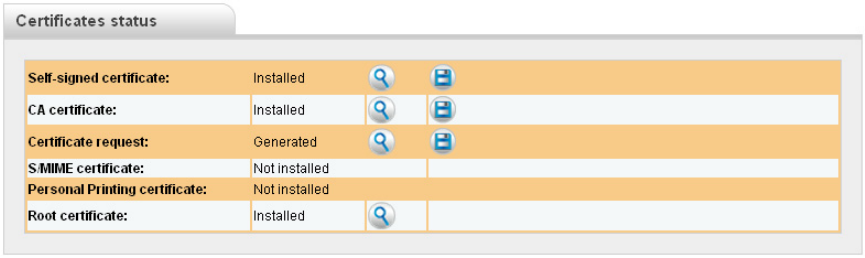


Fig. 6: TPR Control Center - Certificates

What do you want to do?

- ☐ 'Displaying Certificates' ⇨ 70
- ☐ 'Creating a Self-Signed Certificate' ⇨ 70
- ☐ 'Creating a Certificate Request for CA Certificates' ⇨ 71
- ☐ 'Saving the CA Certificate on the TPR' ⇨ 72
- ☐ 'Saving the Root Certificate on the TPR' ⇨ 73
- ☐ 'Saving the pkcs(12) Certificate on the TPR' ⇨ 73
- ☐ 'Saving the S/MIME Certificate on the TPR' ⇨ 74
- ☐ 'Saving the Personal Printing Certificate on the TPR' ⇨ 75
- ☐ 'Deleting Certificates' ⇨ 75

Displaying Certificates

Certificates installed on the TPR and certificate requests can be displayed and viewed.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Select the certificate via the icon* .

The certificate is displayed.

Creating a Self-Signed Certificate

If a self-signed certificate has already been created on the TPR, you must first delete the certificate; see: ⇨ 75.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Click* **Self-signed certificate**.
4. *Enter the relevant parameters, see: Table 14* ⇨ *71.*
5. *Click* **Install**.

↳ The certificate will be created and installed. This may take a few minutes.

Table 14: Parameters for the Creation of Certificates

Parameters	Description
Common name	Is used to clearly identify the certificate. It is advisable to use the IP address or the host name of the TPR to allow a clear assignment of the certificate to the TPR. You can enter a maximum of 64 characters.
Email address	Specifies an email address. You can enter a maximum of 40 characters. (Optional Entry)
Organization name	Specifies the company that uses the TPR. You can enter a maximum of 64 characters.
Organizational unit	Specifies the department or subsection of a company. You can enter a maximum of 64 characters. (Optional Entry)
Location	Specifies the locality where the company is based. You can enter a maximum of 64 characters.
State name	Specifies the state in which the company is based. You can enter a maximum of 64 characters. (Optional Entry)
Domain component	Allows you to enter additional attributes. (Optional Entry)
Country	Specifies the country in which the company is based. Enter the two-digit country code according to ISO 3166. Examples: DE = Germany, GB = Great Britain, US = USA
Issued on	Specifies the date from which on the certificate is valid.
Expires on	Specifies the date from which on the certificate becomes invalid.

Creating a Certificate Request for CA Certificates

As a preparation for the use of a CA certificate, a certificate request that has to be sent to the certification authority can be created in the TPR. The certification authority will then create a CA certificate on the basis of the certificate request. The certificate must be in base 64 format.

If a certificate request has already been created on the TPR, it will be overwritten.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Click* **Certificate request**.
4. *Enter the required parameters, see: Table 14* ⇨ 71.
5. *Click* **Create a request**.
   The creation of the certificate request is in progress. This may take a few minutes.
6. *Select* **Upload** *and save the requests in a text file.*
7. *Click* **OK**.
8. *Send the text file as certificate request to a certification authority.*

When the CA certificate has been received, it must be saved in the TPR; see: ⇨ 72.

Saving the CA Certificate on the TPR

If a CA certificate has already been installed on the TPR, it will be overwritten.

Requirements

☑ A certificate request has been created at an earlier date; see: ⇨ 71.

☑ The certificate must be in base 64 format.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Click* **Requested certificate**.
4. *Click* **Browse**.

5. *Specify the CA certificate.*
6. *Click* **Install**.

↳ The CA certificate is saved in the TPR.

Saving the Root Certificate on the TPR

The TPR offers a number of authentication methods to verify its identity in a network. If you use the authentication method 'EAP-TLS', you must install the root certificate of the authentication server (RADIUS) on the TPR; see: ⇨ 73.

If a root certificate has already been installed on the TPR, it will be overwritten.

Requirements

☑ The certificate must be in base 64 format.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Click* **Root certificate**.
4. *Click* **Browse**.
5. *Specify the root certificate.*
6. *Click* **Install**.

↳ The root certificate is saved in the TPR.

Saving the pkcs(12) Certificate on the TPR

Certificates with the pkcs(12) format are used to save private keys and their respective certificates and to protect them by means of a password.

If a pkcs(12) certificate has already been installed on the TPR, it will be overwritten.

Requirements

☑ The certificate must be in base 64 format.

☑ No certificate request may exist. To delete the certificate request, see: ⇨ 75.

☑ No CA certificate may be installed. To delete a CA certificate, see: ⇨ 75.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Click* **pkcs12 certificate**.
4. *Click* **Browse**.
5. *Specify the pkcs(12) certificate.*
6. *Enter the password.*
7. *Click* **Install**.

↳ The pkcs(12) certificate will be saved in the TPR.

Saving the S/MIME Certificate on the TPR

S/MIME certificates (*.pem file) are used to sign and encrypt the emails that are sent by the TPR.

If an S/MIME certificate has already been installed on the TPR, it will be overwritten.

Requirements

☑ The certificate must be in base 64 format.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Click* **S/MIME certificate**.
4. *Click* **Browse**.
5. *Specify the S/MIME certificate.*
6. *Click* **Install**.

↳ The S/MIME certificate will be saved on the TPR.

Saving the Personal Printing Certificate on the TPR

Personal Printing certificates are used to verify the identity of the Personal Printing server (⇨ 46).

If a Personal Printing certificate has already been installed on the TPR, it will be overwritten.

Requirements

☑ The certificate must be in base 64 format.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Click* **Personal Printing certificate**.
4. *Click* **Browse**.
5. *Specify the Personal Printing certificate.*
6. *Click* **Install**.

↳ The Personal Printing certificate will be saved on the TPR.

Deleting Certificates

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY - Certificates**.
3. *Select the certificate to be deleted via the icon . The certificate is displayed.*
4. *Click* **Delete**.

↳ The certificate is deleted.

7.6 How to Use Authentication Methods

By means of an authentication, a network can be protected against unauthorized access. The TPR can participate in various authentication procedures. This section describes which procedures are supported and how these procedures are configured on the TPR.

What is IEEE 802.1x?

The IEEE 802.1x standard provides a basic structure for various authentication and key management protocols. IEEE 802.1x allows you to control the access to networks. Before users gain access to a network via a network device, they must authenticate themselves in the network. After the authentication was successful, the access to the network will be freed.

What is EAP?

The standard IEEE 802.1x is based upon the EAP (Extensible Authentication Protocol). EAP is a universal protocol for many authentication procedures. EAP allows for a standardized authentication procedure between the network device and an authentication server (RADIUS). First you must define the authentication procedure (TLS, PEAP, TTLS, etc.) to be used and configure it on all network devices involved.

What is RADIUS?

RADIUS (Remote Authentication Dial-In User Service) is an authentication and account management system that validates user login information and grants access to the desired resources.

The TPR supports various EAP authentication methods in order to authenticate itself in a protected network.

What do you want to do?

- ☐ 'Configuring EAP-MD5' ⇨🗎77
- ☐ 'Configuring EAP-TLS' ⇨🗎77
- ☐ 'Configuring EAP-TTLS' ⇨🗎78
- ☐ 'Configuring PEAP' ⇨🗎80
- ☐ 'Configuring EAP-FAST' ⇨🗎81

Configuring EAP-MD5

Benefits and Purpose

EAP-MD5 validates the identity of devices or users before they gain access to network resources. You can configure the TPR for the EAP-MD5 network authentication. This makes sure that the TPR gets access to protected networks.

Mode of Operation

EAP-MD5 describes a user-based authentication method via a RADIUS server. The TPR must be defined as user (with user name and password) on a RADIUS server. The authentication method EAP-MD5 must then be enabled on the TPR and the user name and password need to be entered.

Requirements

☑ The TPR is defined as user (with user name and password) on a RADIUS server.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY – Authentication**.
3. *Select* **MD5** *from the* **Authentication method** *list.*
4. *Enter the user name and the password that are used for the configuration of the TPR on the RADIUS server.*
5. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Configuring EAP-TLS

Benefits and Purpose

EAP-TLS (Transport Layer Security) validates the identity of devices or users before they gain access to network resources. You can configure the TPR for the EAP-TLS network authentication. This makes sure that the TPR gets access to protected networks.

Mode of Operation

EAP-TLS describes a certificate-based authentication method via a RADIUS server. For this purpose, certificates are exchanged between the TPR and the RADIUS server. An encrypted TLS connection between the TPR and the RADIUS server is established in this process. Both RADIUS server and TPR need a valid, digital certificate signed by a CA. The RADIUS server and the print server must validate

the certificate. After the mutual authentication was successful, the access to the network will be freed.

Since each device needs a certificate, a PKI (Public Key Infrastructure) must be available. User passwords are not necessary.

If you want to use the EAP-TLS authentication, you must observe the instructions below in the indicated order. If this procedure is not adhered to, the TPR in the network may not be addressable. In this case you have to reset the TPR parameters; see: ⇨ 87.

Procedure

- Create a certificate request on the TPR; see: 'Creating a Certificate Request for CA Certificates' ⇨ 71.
- Create a CA certificate using the certificate request and the authentication server.
- Install the CA certificate on the TPR; see: 'Saving the CA Certificate on the TPR' ⇨ 72.
- Install the root certificate of the authentication server on the TPR; see: 'Saving the Root Certificate on the TPR' ⇨ 73.
- Enable the authentication method 'EAP-TLS' on the TPR.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY – Authentication**.
3. *Select* **TLS** *from the* **Authentication method** *list.*
4. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Configuring EAP-TTLS

Benefits and Purpose

EAP-TTLS (Tunneled Transport Layer Security) validates the identity of devices or users before they gain access to network resources. You can configure the TPR for the EAP-TTLS network authentication. This makes sure that the TPR gets access to protected networks.

Mode of Operation

EAP-TTLS consists of two phases:

- In phase 1, a TLS-encrypted channel between the TPR and the RADIUS server will be established. Only the RADIUS server authenticates itself on the TPR using a certificate that was signed by a CA. This process is also referred to as 'outer authentication'.
- In phase 2, an additional authentication method is used for the communication within the TLS channel. EAP-defined methods and older methods (CHAP, PAP, MS-CHAP und MS-CHAPv2) are supported. This process is also referred to as 'inner authentication'.

The advantage of this procedure is that only the RADIUS server needs a certificate. Therefore no PKI is needed. Moreover, TTLS supports most authentication protocols.

Requirements

☑ The TPR is defined as user (with user name and password) on a RADIUS server.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY – Authentication**.
3. *Select* **TTLS** *from the* **Authentication method** *list.*
4. *Enter the user name and the password that are used for the configuration of the TPR on the RADIUS server.*
5. *Select the settings intended to secure the communication in the TLS channel.*
6. *To make the connection more secure, you can also install the root certificate of the RADIUS server on the TPR (⇨ 73).*
7. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Configuring PEAP

Benefits and Purpose

PEAP (Protected Extensible Authentication Protocol) validates the identity of devices or users before they gain access to network resources. You can configure the TPR for the PEAP network authentication. This makes sure that the TPR gets access to protected networks.

Mode of Operation

In the case of PEAP (compare EAP-TTLS, see ⇨ 78), an encrypted TLS (Transport Layer Security) channel is established between the TPR and the RADIUS server. Only the RADIUS server authenticates itself on the TPR using a certificate that was signed by a CA.

The TLS channel is then used to establish another connection that can be protected by means of additional EAP authentication methods (e.g. MSCHAPv2).

The advantage of this procedure is that only the RADIUS server needs a certificate. Therefore no PKI is needed. PEAP uses the advantages of TLS and supports various authentication methods, including user passwords and one-time passwords.

Requirements

☑ The TPR is defined as user (with user name and password) on a RADIUS server.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY – Authentication**.
3. *Select* **PEAP** *from the* **Authentication method** *list.*
4. *Enter the user name and the password that are used for the configuration of the TPR on the RADIUS server.*
5. *Select the settings intended to secure the communication in the TLS channel.*
6. *To make the connection more secure, you can also install the root certificate of the RADIUS server on the TPR (⇨ 73).*
7. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Configuring EAP-FAST

Benefits and Purpose

EAP-FAST (Flexible Authentication via Secure Tunneling) validates the identity of devices or users before they gain access to network resources. You can configure the TPR for the EAP-FAST network authentication. This makes sure that the TPR gets access to protected networks.

Mode of Operation

EAP-FAST uses (as in the case of EAP-TTLS, see ⇨ 78) a channel in order to protect the data transfer. The main difference is that EAP-FAST does not require certificates for authentication purposes. (The use of certificates is optional.)

PACs (Protected Access Credentials) are used to build the channel. PACs are credentials that comprise up to three components.

- A shared secret key that contains the preshared key between the TPR and the RADIUS server.
- An opaque element that is provided to the TPR and presented to the RADIUS server when the TPR wishes to obtain access to network resources.
- Other information that may be useful to the client. (Optional)

EAP-FAST uses two methods to generate PACs:

- The manual delivery mechanism can be every mechanism that the administrator configures and considers to be safe for the network.
- In the case of the automatic delivery, an encrypted channel is established in order to protect the authentication of the TPR as well as the delivery of the PACs.

Requirements

☑ The TPR is defined as user (with user name and password) on a RADIUS server.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **SECURITY – Authentication**.
3. *Select* **FAST** *from the* **Authentication method** *list.*
4. *Enter the user name and the password that are used for the configuration of the TPR on the RADIUS server.*
5. *Select the settings intended to secure the communication in the channel.*
6. *Click* **Save & Restart** *to confirm.*

The settings are saved.

7.7 How to Configure a Device Assignment

Man-In-The-Middle Attack

During a man-in-the-middle attack, an invisible attacker joins the communication channel between two communication partners. The attacker can view and manipulate the data traffic.

Protection

You can protect the communication channel between the TPR and the printer by means of a device assignment and thus prevent a man-in-the-middle attack.

During the device assignment, a TPR is permanently assigned to the network printer. The TPR can then only be operated in combination with the assigned network printer. The data traffic cannot be controlled via an intermediate attacker and thus is protected.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **DEVICE – ThinPrint® printer**.
3. *Tick* **Device Assignment**.
4. *Click* **Save & Restart** *to confirm.*

The settings are saved.

8 Maintenance

A number of maintenance activities can be carried out on the TPR. This chapter gives a short overview.

What information do you need?

- 'How to Secure the TPR Parameters (Backup)' ⇨🗎83
- 'How to Use a Connected USB Device' ⇨🗎85
- 'How to Reset Parameters to their Default Values (Reset)' ⇨🗎87
- 'How to Perform an Update' ⇨🗎90
- 'How to Restart the TPR' ⇨🗎91
- 'How to Print a Status or Service Page' ⇨🗎92
- 'How to Display the Job History' ⇨🗎94

8.1 How to Secure the TPR Parameters (Backup)

All parameter values of the TPR (exception: passwords) are saved in the 'parameters' file.

You can save the parameters file as backup copy on your local client. This allows you to get back to a stable configuration status at any time.

You can edit the parameter values of the copied file using a text editor. Afterwards, the configured file can be downloaded to a TPR. The parameter values included in the file will be taken over by the device.

What do you want to do?

- ☐ 'Displaying Parameter Values' ⇨🗎84
- ☐ 'Saving the Parameter File' ⇨🗎84
- ☐ 'Loading the parameters file to a TPR' ⇨🗎84

Displaying Parameter Values

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE - Parameter backup**.
3. *Click the icon* .

The current parameter values are displayed.

A detailed description of the parameters can be found in the 'Parameter List' ⇨100.

Saving the Parameter File

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE - Parameter backup**.
3. *Click the icon* .
   The current parameter values are displayed.
4. *Save the 'parameters' file on a local system with the help of your browser.*

The parameter file is copied and secured.

Loading the parameters file to a TPR

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE - Parameter backup**.
3. *Click* **Browse**.
4. *Specify the 'parameters' file.*
5. *Click* **Import**.

The parameter values in the file are applied to the TPR.

You can also automatically load a parameters file from a USB flash drive to a TPR; see: ⇨ 85.

8.2 How to Use a Connected USB Device

You can connect a USB flash drive to the USB port of the TPR to make use of additional features of the TPR.

Parameter Backup

During the 'parameter backup', the 'parameters' file will be saved automatically on the USB flash drive and updated after a parameter change. The file contains all parameter values of the TPR (exception: passwords). The TPR will automatically take over the values contained in the parameters file on the USB flash drive. This way, the parameter values can be quickly and easily loaded to other TPR via a USB flash drive (e.g. when configuring new devices).

Formatting

To use the USB flash drive on the TPR, the USB flash drive must have the correct file system. You may have to format the USB flash drive, if necessary.

During the formatting process, all data on the USB flash drive will be permanently lost.

Whether formatting is required, will be displayed under 'MAINTENANCE - USB device status' in the TPR Control Center.

What do you want to do?

- ☐ 'Formatting the USB Flash Drive' ⇨ 86
- ☐ 'Saving the Parameter Values Automatically' ⇨ 86
- ☐ 'Loading the Parameter Values Automatically to a TPR' ⇨ 86

Formatting the USB Flash Drive

Requirements

☑ A USB flash drive has been connected to the TPR.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE – USB device**.
3. *Click* **Formatting**.

↳ The USB flash drive will be formatted.

Saving the Parameter Values Automatically

Requirements

☑ A USB flash drive has been connected to the TPR.

☑ The USB flash drive has been formatted correctly; see: ⇨ 86.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE – USB device**.
3. *Tick* **Parameter backup**.
4. *Click* **Save & Restart**.

↳ The settings are saved.

Loading the Parameter Values Automatically to a TPR

Requirements

☑ The USB flash drive has been formatted correctly; see: ⇨ 86.

☑ A parameter file exists on the USB flash drive; see 'Parameter Backup' ⇨ 85.

Proceed as follows:

1. *Connect a USB flash drive to the USB port of the TPR.*

↳ The parameter values in the file are automatically applied to the TPR.

8.3 How to Reset Parameters to their Default Values (Reset)

It is possible to reset the parameters of the TPR to their default values (factory settings). All previously configured parameter values will be deleted in this process. Installed certificates will not be deleted.

If you reset the parameters, the IP address of the TPR may change and the connection to the TPR Control Center may be terminated.

You must reset the parameters, for example, if you have changed the location of the TPR and if you want to use the TPR in a different network. Before this change of location, you should reset the parameters to the default settings to install the TPR in another network.

Remove an attached USB flash drive before resetting the parameters. If a parameters file is saved on the USB flash drive, the TPR will - after the reset - automatically use the parameter values saved on the USB flash drive (see: ⇨ 85).

By means of the status/reset button of the device you can reset the parameters without entering the password.

What do you want to do?

- ☐ 'Resetting the Parameters via the TPR Control Center' ⇨ 87
- ☐ 'Resetting Parameters via the InterCon-NetTool' ⇨ 88
- ☐ 'Resetting the parameters via the status/reset button' ⇨ 88

Resetting the Parameters via the TPR Control Center

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE - Default settings.**

3. *Click* **Default settings**.

↳ The parameters are reset.

Resetting Parameters via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Highlight the TPR in the device list.*
3. *Select* **Actions – Default Settings** *from the menu bar.*
4. *Click* **Finish**.

↳ The parameters are reset.

Resetting the parameters via the status/reset button

LEDs, various ports and the status/reset button can be found on the TPR. These components are described in the 'Quick Installation Guide'.

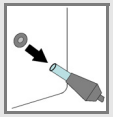
Using the status/reset button you can reset the parameter values of the TPR to their default settings. The reset process can be divided into three phases.

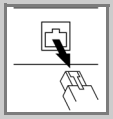
- During phase one, the TPR is forced into the reset mode. During the reset mode, the parameters are reset.
- The second phase describes the restart of the device.
- The third phase describes the printing of a status page. The reset process can be checked by means of the status page.

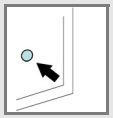
IMPORTANT: The reset mode is indicated by the green and red blinking of the activity LED. The activity LED will then blink orange.
You must release the status/reset button at this moment, otherwise the TPR switches to the BIOS mode. If this happens, try the reset again.

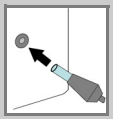
The phases are described in the following:

[Phase 1] Reset

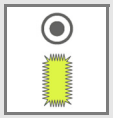

Turn off the TPR
(interrupt the power supply).


Remove the network cable
(RJ-45) from the TPR.

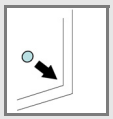

Press and hold the status/reset button.


Turn on the TPR
(establish the power supply).

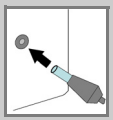
The activity LED will then be permanently lit in orange.


After a few seconds, the activity LED will alternatingly blink green and red.

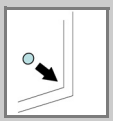
Wait until the activity LED will blink orange.


Release the status/reset button for about 1 second.

The activity LED alternatingly blinks green and red.

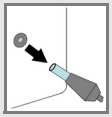

Press and hold the status/reset button again.

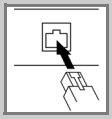
The activity LED blinks orange twice.

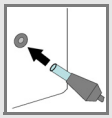

Release the status/reset button.

The activity LED blinks green.

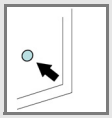
[Phase 2] Restart of the device


Turn off the TPR
(interrupt the power supply).


Connect the network cable
(RJ-45) to the TPR.


Turn on the TPR
(establish the power supply).

[Phase 3] Status check


Press and hold the status/reset button for a short time.

The status page is printed.

8.4 How to Perform an Update

You can carry out software and firmware updates on the TPR. Updates allow you to benefit from currently developed features.

What Happens during an Update?

In the course of an update, the old firmware/software will be overwritten and replaced by the new firmware/software. The parameter default settings of the device remain unchanged.

When is an Update recommended?

An update should be undertaken if function do not work properly and if SEH Computertechnik GmbH has released a new software or firmware version with new functions or bug fixes.

Check the installed software and firmware version on the TPR. You will find the version number on the TPR Control Center homepage or in the product list in the InterCon-NetTool.

Where do I Find the Update Files?

Current firmware and software files can be downloaded from the homepage of SEH Computertechnik GmbH:

http://www.seh-technology.com/services/downloads/tpr.html

Every update file has its own 'readme' file. Take note of the information contained in the 'readme' file.

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE – Update**.
3. *Click* **Browse**.
4. *Select the update file.*
5. *Click* **Install**.

The update is executed. The TPR will be restarted.

8.5 How to Restart the TPR

The TPR is rebooted automatically after parameter changes or updates. If the TPR is in an undefined state it can also be rebooted manually.

What do you want to do?

- ☐ 'Rebooting the TPR via the TPR Control Center' ⇨📄91
- ☐ 'Restarting the TPR via the InterCon-NetTool' ⇨📄91

Rebooting the TPR via the TPR Control Center

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE - Restart**.
3. *Click* **Restart**.

The TPR will be restarted.

Restarting the TPR via the InterCon-NetTool

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Highlight the TPR in the device list.*
3. *Select* **Actions – Restart** *from the menu bar.*
   The **Restart print server** *dialog appears.*
4. *Click* **Finish**.

The TPR will be restarted.

8.6 How to Print a Status or Service Page

You can print status or service pages to the connected network printer. Both pages are available in English.

Status Page

A status page contains basic information of the TPR such as the model type, hardware address, IP address, subnet mask, gateway, etc.

Service page

A service page contains basic information of the TPR as well as a list of the current parameter values of the TPR.

Before a status or service page is printed, the printing function must be enabled and the data format of the status or service page (ASCII, PostScript, DATAMAX or Citizen-Z) must be specified. ASCII is preset as data format.

What do you want to do?

- ☐ 'Specifying the Printing Function and the Data Format via the TPR Control Center' ⇨ 92
- ☐ 'Printing a Status Page via the TPR Control Center' ⇨ 93
- ☐ 'Printing a Status Page via the Status/Reset Button' ⇨ 93
- ☐ 'Printing a Service Page via the TPR Control Center' ⇨ 93
- ☐ 'Printing a Service Page via the Status/Reset Button' ⇨ 93

Specifying the Printing Function and the Data Format via the TPR Control Center

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE – Status page**.
3. *Select the desired data format from the* **Status page mode** *list.*
4. *Tick* **Printing**.
5. *Click* **Save & Restart** *to confirm.*

The settings are saved.

Printing a Status Page via the TPR Control Center

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE – Status page**.
3. *Click* **Status page**.

The status page is printed.

Printing a Status Page via the Status/Reset Button

You can print a status page via the status/reset button of the device.

Proceed as follows:

1. *Press the status/reset button for a short time.*

The status page is printed.

Printing a Service Page via the TPR Control Center

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE – Status page**.
3. *Click* **Service page**.

The service page will be printed.

Printing a Service Page via the Status/Reset Button

You can print a service page via the status/reset button of the device.

Proceed as follows:

1. *Keep the status/reset button pressed for five seconds.*

The status page is printed.

8.7 How to Display the Job History

You can get information about the ThinPrint print jobs that have been sent to the TPR. Only these print jobs are registered and shown in the job history.

A time server (⇨📄36) must be configured on the TPR so that the date and time can be displayed correctly. If no time server is configured, the time stamp corresponds to the default time.

A maximum of 32 print jobs are displayed. The first-in, first-out method is applied from the 33rd print job onwards. The saved print jobs will be deleted when the TPR is turned off or reset. The print jobs can also be deleted manually. The print jobs will not be deleted when the TPR is restarted.

What do you want to do?

- ☐ 'Displaying the job history' ⇨📄94
- ☐ 'Deleting Print Jobs Manually' ⇨📄95

Displaying the job history

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE - Job history**.

↳ The Job History is displayed.

The following information is shown in the Job History:

Information	Description
ID	Identification number of the printer that has spooled the print job.

Information	Description
Status	Status of the print connection. The following statuses are possible: • 'Initialized' means that there is a connection to the ThinPrint server. In a next step, the connection to the printer will be established. • 'Try to connect' means that the connection to the printer will be established. • 'Connection rejected' means that the printer rejected the connection. • 'Pending' means that the print job has been accepted by the TPR but that the data transfer has not yet started. • 'Processing' means that the print job has been transferred from the TPR to the printer. • 'Processing stopped' means that the data transfer to the printer was interrupted. This can occur if, for example, the printer ran out of paper. If the printer error is fixed, data transfer will be resumed. • 'Completed' means that the TPR has completely forwarded the print job to the printer. • 'Aborted' means that the print job has been aborted. This can occur if, for example, the TPR has been restarted while the print job was processed.
Protocol	Protocol used to transfer the print data. The presentation consists in a combination of the following values: • 'ThP' - ThinPrint • 'Stp' - status or service page • 'Sock' - RAW/Socket printing • 'IPP' - IPP printing • 'LPD' - LPD printing
Name	Name of the print job
Sender	Name of the sending host: • '<domain user name>@<domain>' appears with ThinPrint print jobs. • 'TPR-10' appears when printing a status or service page.
Start	Time at which the print job has been sent to the TPR.
Size	Size (in Kb) of the print job.
Duration	The time needed by the TPR for processing the print job.

Deleting Print Jobs Manually

Proceed as follows:

1. *Start the TPR Control Center.*
2. *Select* **MAINTENANCE - Job history.**
3. *Click* **Delete.**

All print jobs listed in the job history will be deleted.

9 Appendix

The appendix contains a glossary, the TPR parameter list, a trouble shooting and the index lists of this document.

What information do you need?

- 'Glossary' ⇨📄97
- 'Parameter List' ⇨📄100
- 'Troubleshooting' ⇨📄120
- 'List of Figures' ⇨📄123
- 'Index' ⇨📄124

9.1 Glossary

The glossary contains information about manufacturer-specific software solutions and terms from the world of network technology.

What information do you need?

Manufacturer-Specific Software Solutions

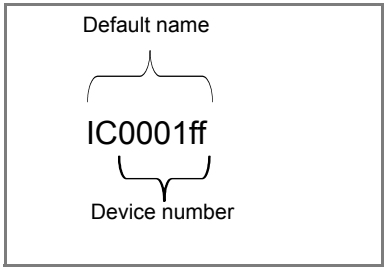
- 'InterCon-NetTool' ⇨📄99
- 'TPR Control Center' ⇨📄99

Network Technology

- 'Default Name' ⇨📄97
- 'Gateway' ⇨📄98
- 'Hardware Address' ⇨📄98
- 'Host Name' ⇨📄98
- 'IP Address' ⇨📄99
- 'Subnet Mask' ⇨📄99

Default Name

The default name of the TPR is made up of the two letters 'IC' and the device number. The device number consists of the last six numbers of its hardware address.



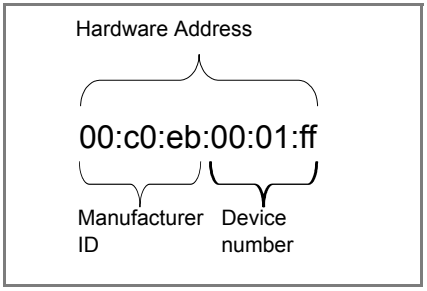
The default name can be found in the TPR Control Center, the InterCon-NetTool, on the status or service page.

Gateway

Using a gateway, you can address IP addresses from external networks. If you wish to use a gateway, you can configure the relevant parameter via the TPR Control Center or the InterCon-NetTool.

Hardware Address

The TPR is addressable by means of its world-wide unique hardware address. This address is commonly referred to as the MAC or Ethernet address. The manufacturer has defined this address in the hardware of the device. The address consists of 12 hexadecimal numbers. The first six numbers represent the manufacturer, while the last six numbers identify the individual device.



The hardware address can be found on the housing, the InterCon-NetTool, the status or service page.

The use of separators within the hardware address depends on the platform. Note the following conventions when entering the hardware address:

Operating system	Representation	Example
Windows	Hyphen	00-c0-eb-00-01-ff
UNIX	Colon or period	00:c0:eb:00:01:ff or 00.c0.eb.00.01.ff

Host Name

The host name is an alias for an IP address. The host name uniquely identifies the TPR in the network and makes it easier to remember.

InterCon-NetTool

The software InterCon-NetTool has been developed by SEH Computertechnik GmbH for the administration of SEH network devices within a predefined network.

IP Address

The IP address is the unique address of each node in a network, i.e. an IP address may occur only once on a local network. The system administrator usually assigns the IP address. The address must be saved in the TPR to make sure that it can be addressed within the network.

Subnet Mask

With the help of the subnet mask, large networks can be split up into subnetworks. In this case, the user IDs of the IP addresses are assigned to the various subnetworks.

By default, the TPR is configured for the use without subnetworks. If you wish to use a subnetwork, you can configure the relevant parameter via the TPR Control Center or the InterCon-NetTool.

TPR Control Center

The TPR can be configured and monitored via the TPR Control Center. The TPR Control Center is stored in the TPR and can be displayed by means of a browser software (Internet Explorer, Firefox, Safari).

9.2 Parameter List

This chapter gives an overview of all parameters of the TPR. The parameter list gives details about the functions and values of the individual parameters.

What information do you need?

- 'Parameter List - IPv4' ⇨🗎101
- 'Parameter List – IPv6' ⇨🗎101
- 'Parameter List - DNS' ⇨🗎102
- 'Parameter List - SNMP' ⇨🗎103
- 'Parameter List - POP3' ⇨🗎104
- 'Parameter List - SMTP' ⇨🗎105
- 'Parameter List - Bonjour' ⇨🗎106
- 'Parameter List - Date/Time' ⇨🗎106
- 'Parameter List - Description' ⇨🗎106
- 'Parameter List - TPR-10' ⇨🗎107
- 'Parameter List - Local Service Ports' ⇨🗎108
- 'Parameter List - Personal Printing' ⇨🗎109
- 'Parameter List - ThinPrint®' ⇨🗎111
- 'Parameter List - ThinPrint Connection Service' ⇨🗎112
- 'Parameter List - ThinPrint® printer' ⇨🗎113
- 'Parameter List - Notification' ⇨🗎114
- 'Parameter List - SSL connections' ⇨🗎116
- 'Parameter List - Web access' ⇨🗎116
- 'Parameter List – Port Blocking' ⇨🗎116
- '' ⇨🗎117
- 'Parameter List - Authentication' ⇨🗎118
- 'Parameter List - USB device' ⇨🗎119
- 'Parameter List – Status page' ⇨🗎119

To view the current parameter values of your TPR, see: 'Displaying Parameter Values' ⇨84 and 'How to Print a Status or Service Page' ⇨92.

Table 15: Parameter List - IPv4

Parameters	Value	Default	Description
ip_dhcp [DHCP]	on/off	on	Enables/disables the DHCP protocol.
ip_bootp [BOOTP]	on/off	on	Enables/disables the BOOTP protocol.
ip_auto [ARP/PING]	on/off	on	Enables/disables the IP address assignment via ARP/PING.
ip_addr [IP address]	valid IP address	169.254.0.0/16	Defines the IP address of the TPR.
ip_mask [Subnet mask]	valid IP address	255.255.0.0	Defines the subnet mask of the TPR.
ip_gate [Gateway]	valid IP address	0.0.0.0	Defines the gateway address of the TPR.

Table 16: Parameter List – IPv6

Parameters	Value	Default	Description
ipv6 [IPv6]	on/off	on	Enables/disables the IPv6 functionality of the TPR.
ipv6_auto [Automatic configuration]	on/off	on	Enables/disables the automatic assignment of the IPv6 address for the TPR.

Parameters	Value	Default	Description
ipv6_addr [IPv6 address]	n:n:n:n:n:n:n:n	: :	Defines a manually assigned IPv6 Unicast address in the n:n:n:n:n:n:n:n format for the TPR. *Every 'n' represents the hexadecimal value of one of the eight 16 bit elements of the address. An IPv6 address may be entered or displayed using a shortened version when successive fields contain all zeros (0). In this case, two colons (::) are used.*
ipv6_gate [Router]	n:n:n:n:n:n:n:n	: :	Defines the IPv6 unicast address of the router. The TPR sends its 'Router Solicitations' (RS) to this router.
ipv6_plen [Prefix length]	0 - 64 [2 characters; 0-9]	64	Defines the length of the subnet prefix for the IPv6 address. *Address ranges are indicated by prefixes. The prefix length (number of bits used) is added to the IPv6 address and specified as a decimal number. The decimal number is separated by '/'.*

Table 17: Parameter List - DNS

Parameters	Value	Default	Description
dns [DNS]	on/off	on	Enables/disables the name resolution via a DNS server.
dns_primary [Primary DNS server]	valid IP address	0.0.0.0	Defines the IP address of the primary DNS server.
dns_secondary [Secondary DNS server]	valid IP address	0.0.0.0	Defines the IP address of the secondary DNS server. *The secondary DNS server is used if the primary DNS server is not available.*

Parameters	Value	Default	Description
dns_domain [Domain name (suffix)]	max. 255 characters [., a-z, A-Z, 0-9]	[blank]	Defines the domain name of an existing DNS server.

Table 18: Parameter List - SNMP

Parameters	Value	Default	Description
snmpv1 [SNMPv1]	on/off	on	Enables/disables SNMPv1.
snmpv1_ronly [Read-only]	on/off	off	Enables/disables the write protection for the community.
snmpv1_community [Community]	max. 64 characters [a-z, A-Z, 0-9]	public	Defines the name of the SNMP community. *The SNMP community is a basic form of access protection in which several participants with the same access rights are grouped together.*
snmpv3 [SNMPv3]	on/off	on	Enables/disables SNMPv3.
any_name [User name]	max. 64 characters [a-z, A-Z, 0-9]	anonymous	Defines the name of the SNMP user group 1.
any_pwd [Password]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the password of the SNMP user group 1.
any_hash [Hash]	md5 sha	md5	Specifies the hash algorithm of the SNMP user group 1.
any_rights [Access rights]	--- [None] readonly readwrite	readonly	Defines the access rights of the SNMP user group 1.
any_cipher [Encryption]	--- [None] aes des	---	Defines the encryption method of the SNMP user group 1.
admin_name [User name]	max. 64 characters [a-z, A-Z, 0-9]	admin	Defines the name of the SNMP user group 2.
admin_pwd [Password]	8 - 64 characters [a-z, A-Z, 0-9]	administrator	Defines the password of the SNMP user group 2.

Parameters	Value	Default	Description
admin_hash [Hash]	md5 sha	md5	Specifies the hash algorithm of the SNMP user group 2.
admin_rights [Access rights]	--- [None] readonly readwrite	readwrite	Defines the access rights of the SNMP user group 2.
admin_cipher [Encryption]	--- [None] aes des	---	Defines the encryption method of the SNMP user group 2.

Table 19: Parameter List - POP3

Parameters	Value	Default	Description
pop3 [POP3]	on/off	off	Enables/disables the POP3 functionality.
pop3_srv [Server name]	max. 128 characters	[blank]	Defines the name of the POP3 server.
pop3_port [Server port]	1-65535 [max. 5 characters; 0-9]	110	Defines the port of the POP3 server used by the TPR for receiving emails. *When using SSL/TLS, enter 995 as port number.*
pop3_sec [Security]	0 = --- [no security] 1 = APOP 2 = SSL/TLS	0	Defines the authentication method to be used.
pop3_poll [Check mail every]	1-10080 [max. 5 characters; 0-9]	15	Defines the time interval (in minutes) for retrieving emails from the POP3 server.
pop3_limit [Ignore mail exceeding]	0-4096 [max. 4 characters; 0-9; 0 = unlimited]	10	Defines the maximum email size (in Kbyte) to be accepted by the TPR.
pop3_usr [User name]	max. 128 characters	[blank]	Defines the name used by the TPR to log on to the POP3 server.
pop3_pwd [Password]	max. 128 characters	[blank]	Defines the password used by the TPR to log on to the POP3 server.

Table 20: Parameter List - SMTP

Parameters	Value	Default	Description
smtp_srv [Server name]	max. 128 characters	[blank]	Defines the name of the SMTP server.
smtp_port [Server port]	1-65535 [max. 5 characters; 0-9]	25	Defines the port number used by the TPR to send emails to the SMTP server.
smtp_ssl [TLS]	on/off	off	Enables/disables TLS. *The security protocol TLS (Transport Layer Security) is used to encrypt the transmission between the TPR and the SMTP server.*
smtp_sender [Sender name]	max. 128 characters	[blank]	Defines the email sender name to be used by the TPR.
smtp_auth [Login]	on/off	off	Enables/disables the SMTP authentication for the login.
smtp_usr [User name]	max. 128 characters	[blank]	Defines the name used by the TPR to connect to the SMTP server.
smtp_pwd [Password]	max. 128 characters	[blank]	Defines the password used by the TPR to connect to the SMTP server.
smtp_sign [Security (S/MIME)]	on/off	off	Enables/disables the encryption and signing of emails via S/MIME.
smtp_encrypt [Full encryption] [Signing of emails]	on/off [off = sign, on = encrypt]	off	Defines the signing and encryption of emails.
smtp_attpkey [Attach public key]	on/off	on	Enables/disables the attachment of a public key to an email.

Table 21: Parameter List - Bonjour

Parameters	Value	Default	Description
bonjour [Bonjour]	on/off	on	Enables/disables the Bonjour service.
bonjour_name [Bonjour name]	max. 64 characters [a-z, A-Z, 0-9]	[Default Name]	Defines the Bonjour name of the TPR.

Table 22: Parameter List - Date/Time

Parameters	Value	Default	Description
ntp [Date/Time]	on/off	on	Enables/disables the use of a time server (SNTP).
ntp_server [Time server]	max. 255 characters [., a-z, A-Z, 0-9]	pool.ntp.org	Defines a time server via the IP address or the host name. *(A host name can only be used if a DNS server was configured beforehand.)*
ntp_tzone [Time zone]	UTC, GMT, EST, EDT, CST, CDT, MST, MDT, PST, PDT, etc.	CET/CEST (EU)	The time zone is used to equalize the difference between the time received over the time server and the local time.

Table 23: Parameter List - Description

Parameters	Value	Default	Description
sys_name [Host name]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the host name of the TPR.
sys_descr [Description]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Freely definable description (of the TPR).
sys_contact [Contact person]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Freely definable description (of the contact person).

Table 24: Parameter List - TPR-10

Parameters	Value	Default	Description
nat_local [Local IP address]	valid IP address	192.168. 156.156/ 28	Defines the IP address of the TPR for the internal communication. *The TPR and printer constitute an internal IP network. The local IP address is the gateway to the printer IP address. The subnet mask is 255.255.255.240.*
nat_remote [Printer IP address]	valid IP address	192.168. 156.157/ 28	Defines the IP address of the printer for the internal communication. *The TPR and printer constitute an internal IP network. The printer IP address and related parameters are set by the internal DHCP server of the TPR.*
nat_src [Masquerading]	on/off	off	Enables/disables masquerading. *Masquerading is a type of NAT (Network Address Translation). In NAT, all external IP addresses are translated to the local IP address.*
nat_icmp [ICMP]	on/off	on	Enables/disables the routing of ICMP packets to the printer IP address. *In IP networks, ICMP is used to transmit error messages and queries, for example 'ping'. If the option is enabled, queries will be answered by the printer and not by the TPR.*

Table 25: Parameter List - Local Service Ports

Parameters	Value	Default	Description
httpd_port [HTTP]	1-65535 [max. 5 characters; 0-9]	80	Defines the TCP port that is used by the TPR for HTTP during the network communication.
httpsd_port [HTTPS]	1-65535 [max. 5 characters; 0-9]	443	Defines the TCP port that is used by the TPR for HTTPS during the network communication.
snmp_port [SNMP]	1-65535 [max. 5 characters; 0-9]	161	Defines the TCP port that is used by the TPR for SNMP during the network communication.
tpgPort [ThinPrint®]	1-65535 [max. 5 characters; 0-9]	4000	Defines the TCP port used by the TPR for communicating with the ThinPrint® server.

Table 26: Parameter List - Personal Printing

Parameters	Value	Default	Description
pps [Personal Printing]	on/off	on	Enables/disables the Personal Printing functionality of the TPR.
pps_server [Server name]	max. 255 characters [., a-z, A-Z, 0-9]	[blank]	Defines a Personal Printing server via the IP address or the host name. *(A host name can only be used if a DNS server was configured beforehand.)*
pps_port [Server port]	1-65535 [max. 5 characters; 0-9]	80	Defines the TCP port used by the TPR for communicating with the Personal Printing server. *If the SSL connection is enabled, the port number 443 must be used.*
pps_ssl [SSL connection]	on/off	off	Enables/disables the SSL/TLS encryption and certificate-based authentication for the Personal Printing protocol.
pps_verify [Verify certificate]	on/off	off	Enables/disables the verification of the Personal Printing server certificate by means of the root certificate and/or the Personal Printing certificate.
pps_pwd [User-PIN]	max. 32 characters	SEH	Defines the User-PIN. The specified User-PIN and the User-PIN in the user accounts of the Active Directory must be identical.
pps_prtID [Printer ID]	0-64 [max. 2 characters; 0-9]	1	Defines the ID of the printer object to be used by the Personal Printing server.
pps_single [Trigger print jobs separately]	on/off	on	Enables/disables the release of one single print job per cardswipe. If several print jobs are available, they have to be released individually one after another.

Parameters	Value	Default	Description
pps_delete [Job deletion by server]	on/off	on	Enables/disables the immediate deletion of printed jobs by the Personal Printing server. *This setting will override any settings for the deletion of printed jobs set on the Personal Printing server. If neither the job deletion by server nor the job deletion by TPR is enabled, printed jobs will be deleted as defined in the settings on the Personal Printing server.*
pps_extraDel [Job deletion by TPR]	on/off	off	Enables/disables the deletion of printed jobs by the TPR. The time of deletion can be defined via the delay. *This setting will override any settings for the deletion of printed jobs set on the Personal Printing server. If neither the job deletion by server nor the job deletion by TPR is enabled, printed jobs will be deleted as defined in the settings on the Personal Printing server.*
pps_wait2Del [Delay]	0 - 60 [max. 2 characters; 0-9; 0 = immediate deletion]	0	Defines a delay (in seconds) for the deletion of printed jobs by the TPR. A delay assures the complete transfer to the printer and printout of the print job.
pps_beep [Beeper]	on/off	on	Enables/disables the audio feedback. Audio signals give information about the triggering of print jobs.

Table 27: Parameter List - ThinPrint®

Parameters	Value	Default	Description
tpgPort [ThinPrint® port]	1 - 65535 [max. 5 characters; 0-9]	4000	Defines the TCP port used by the TPR for communicating with the ThinPrint server.
tpgBdwidth [Bandwidth]	on/off	off	Enables/disables the bandwidth functionality of the ThinPrint® port (TPR side).
tpgBdwidthVal [Bandwidth value]	1600 - 1000000 [at least 4 characters, max. 7 characters; 0-9]	256000	Defines the bandwidth (in bit/second) used to decrease the bandwidth of the ThinPrint® port (TPR side).
tpgPrtoToVal [Printer connection timeout]	0 - 86400 [max. 5 characters; 0-9; 0 = off]	60	Defines the period of time (in seconds) after which a connection attempt to a printer is aborted. *A connection attempt should be aborted if a printer is physically not available. This frees the ThinPrint® port for subsequent print jobs.*
tpgJobSndTout [Job sending timeout]	0 - 86400 [max. 5 characters; 0-9;; 0 = off]	180	Defines the period of time (in seconds) after which a current print job is aborted if it cannot be printed due to a printer error, e.g. no paper.

Table 28: Parameter List - ThinPrint Connection Service

Parameters	Value	Default	Description
conService [Connection Service]	on/off	off	Enables/disables the ThinPrint Connection Service.
conServer [Server name]	max. 255 characters [., a-z, A-Z, 0-9]	[blank]	Defines the Connection Service server via the IP address or the host name. *(A host name can only be used if a DNS server was configured beforehand.)*
tpgClientID [Client ID]	0 - 99999 [max. 5 characters; 0-9]	0	Defines the client ID as stored in the database of the ThinPrint® Connection Service.
tpgAuthKey [Authentication key]	0 - 99999 [max. 5 characters; 0-9]	0	Defines the authentication key as stored in the database of the Connection Service.
conPort [Port]	1 - 65535 [max. 5 characters; 0-9]	4001	Defines the TCP port used by the TPR for communicating with the Connection Service.
tpgKeepalive [Keep alive]	1 - 60000 [max. 5 characters; 0-9]	60	Defines the time interval (in seconds) after which the connection to the Connection Service is refreshed. *Note: The value has to be equal to or lower than the 'KeepAliveTO' value set on the Connection Service server.*
tpgRetry [Connection retry]	1 - 60000 [max. 5 characters; 0-9]	120	Defines the time interval (in seconds) after which a connection retry is executed if the Connection Service cannot be reached.

Table 29: Parameter List - ThinPrint® printer

Parameters	Value	Default	Description
prtName_1 [Printer]	max. 32 characters [a-z, A-Z, 0-9, _, -]	[blank]	Defines the printer name for the ThinPrint AutoConnect feature.
prtClass_1 [Class]	max. 7 characters [a-z, A-Z, 0-9]	[blank]	Defines the printer class name for the ThinPrint AutoConnect feature.
prtDriver_1 [Driver]	max. 64 characters [a-z, A-Z, 0-9, _, -]	[blank]	Defines the printer driver for the ThinPrint AutoConnect feature.
remoteMode_1 [Printing protocol]	raw = RAW/Socket connection ipp = IPP connection lpd = LPD connection	raw	Specifies the transfer method between the TPR and the printer.
remotePort_1 [Port]	1 - 65535 [max. 5 characters; 0-9]	9100	Defines the port number for RAW/socket printing.
remoteUrl_1 [URL]	max. 64 characters	ipp/lp1	Specifies the second part of the printer URL for IPP printing. *The implementation of the printer URL is depends on the manufacturer. Consult your printer manual for more information.*
remoteIPPs_1 [SSL]	on/off	off	Enables/disables the SSL/TLS encryption for IPP printing.
remoteQ_1 [Queue]	max. 64 characters [a-z, A-Z, 0-9]	lp1	Defines the queue name for LPD printing.
lpdModeRFC_1 [RFC]	on/off	on	Enables/disables the RFC1179 conformity for LPD printing.
monitorPing [Monitoring via ping]	on/off	on	Enables/disables monitoring via 'ping', i.e. ICMP. *The 'ping' query allows you to view the printer availability.*

Parameters	Value	Default	Description
monitorSNMP [SNMP]	on/off	on	Enables/disables monitoring via SNMP. *The SNMP query shows printer messages.*
monitorPoll [Monitoring interval]	1 - 86400 [max. 5 characters; 0-9]	30	Defines the interval of a 'ping' or 'SNMP' query in seconds.
prtLock [Device assignment]	on/off	off	Enables/disables the printer assignment. The TPR can be permanently assigned to the printer. The TPR can then only be operated together with the assigned printer.

Table 30: Parameter List - Notification

Parameters	Value	Default	Description
mailto_1 mailto_2 [Mail recipient]	valid email address [max. 64 characters]	[blank]	Defines the email address of the recipient for notifications.
noti_pup_1 noti_pup_2 [Restart]	on/off	off	Enables/disables the sending of emails when the TPR is restarted.
noti_stat_1 noti_stat_2 [Status]	on/off	off	Enables/disables the periodical sending of a status email to recipient 1 or 2.
notistat_d [Interval]	al = daily su = Sunday mo = Monday tu = Tuesday we = Wednesday th = Thursday fr = Friday sa = Saturday	al	Specifies the interval at which a status email is sent.
notistat_h [hh]	1 = 1. Hour 2 = 2. Hour 3 = 3. Hour etc.	0	Specifies the time at which a status email is sent.

Parameters	Value	Default	Description
notistat_tm [mm]	0 = 00 min 1 = 10 min 2 = 20 min 3 = 30 min 4 = 40 min 5 = 50 min 6 = 00 min	0	Specifies the time at which a status email is sent.
noti_card_1 noti_card_2 [Cards]	on/off	off	Enables/disables the sending of emails/traps if a card event occurs at the TPR.
noti_usb_1 noti_usb_2 [USB]	on/off	off	Enables/disables the sending of emails after a USB flash drive was connected to or removed from the TPR.
noti_err_1 noti_err_2 [Problems]	on/off	off	Enables/disables the sending of emails if a problem occurs at the TPR.
trapto_1 trapto_2 [Trap target]	valid IP address	0.0.0.0	Defines the SNMP trap address of the recipient for notifications.
trapcommu_1 trapcommu_2 [Trap community]	max. 64 characters [a-z, A-Z, 0-9]	public	Defines the SNMP trap community of the recipient.
trappup [Restart]	on/off	off	Enables/disables the sending of SNMP traps when the TPR is restarted.
trapcard [Cards]	on/off	off	Enables/disables the sending of emails/traps if a card event occurs at the TPR.
trapusb [USB]	on/off	off	Enables/disables the sending of SNMP traps after a USB flash drive was connected to or removed from the TPR.
traperr [Problems]	on/off	off	Enables/disables the sending of SNMP traps if a problem occurs at the TPR.

Tabelle 31: Parameter List - SSL connections

Parameter	Value	Default	Description
security [Encryption]	1 - 4 [1 character]	2	Defines the encryption level to be used for SSL/TLS connections. *1 = Low (56 bit)* *2 = Medium (128 bit)* *3 = High (128 - 256 bit)* *4 = Compatible (40- 256 bit)*

Table 32: Parameter List - Web access

Parameters	Value	Default	Description
http_allowed [HTTP/HTTPS]	on/off	on	Defines the permitted type of connection (HTTP/HTTPS) to the TPR Control Center. *If HTTPS is exclusively chosen as the connection type [http_allowed = off], the administrative access to the TPR Control Center is protected via SSL/TLS.*
http_pwd [Password]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the password for the administrative access to the TPR Control Center.

Table 33: Parameter List – Port Blocking

Parameters	Value	Default	Description
drop_port_1 ~ drop_port_12 [Port]	1 - 65535 [max. 5 characters; 0-9]	0	Defines the port number of the port to be blocked. A total of 12 ports can be blocked.
drop_tcp_1 ~ drop_tcp_12 [TCP]	on/off	off	Blocks the access to selected TCP ports. *TCP and UDP ports can be blocked at the same time.*

Parameters	Value	Default	Description
drop_udp_1 ~ drop_udp_12 [UDP]	on/off	off	Blocks the access to selected UDP ports. *TCP and UDP ports can be blocked at the same time.*
drop_lan_1 ~ drop_lan_12 [LAN]	on/off	off	Blocks the access to selected LAN interfaces (network connection). *Printer and LAN interfaces can be blocked at the same time.*
drop_nat_1 ~ drop_nat_12 [Printer]	on/off	off	Blocks the access to selected printer interfaces (printer connection). *Printer and LAN interfaces can be blocked at the same time.*

Table 34: Parameter List - TCP port access

Parameters	Value	Default	Description
protection [Port access control]	on/off	off	Enables/disables the locking of the selected ports.
protection_test [Test mode]	on/off	on	Enables/disables the test mode. *The test mode allows you to test the parameters set using the access control. If the test mode is activated, the access protection remains active until the TPR is rebooted.*
protection_level [Security level]	protec_tcp protec_all	protec_tcp	Specifies the port types to be locked: - TCP ports - all ports (IP ports)
ip_filter_on_1 ~ ip_filter_on_8 [IP address]	on/off	off	Enables/disables an exception from the port locking.
ip_filter_1 ~ ip_filter_8 [IP address]	valid IP address	[blank]	Defines elements that are excluded from port locking, using the IP address.

Parameters	Value	Default	Description
hw_filter_on_1 ~ hw_filter_on_8 [MAC address]	on/off	off	Enables/disables an exception from the port locking.
hw_filter_1 ~ hw_filter_8 [MAC address]	valid hardware address	00:00:00 :00:00:0 0	Defines elements that are excluded from port locking, using the hardware address.

Table 35: Parameter List - Authentication

Parameters	Value	Default	Description
auth_typ [Authentication method]	--- [None] MD5 TLS TTLS PEAP FAST	----	Defines the authentication method that is used to identify devices or users in the network.
auth_name [User name]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the name of the TPR as saved in the authentication server (RADIUS).
auth_pwd [Password]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the password of the TPR as saved in the authentication server (RADIUS).
auth_extern [PEAP/EAP-FAST Options]	--- [None] PEAPLABEL0 PEAPLABEL1 PEAPVER0 PEAPVER1 FASTPROV1	---	Defines the kind of external authentication for the EAP authentication methods TTLS, PEAP, and FAST.
auth_intern [Inner Authentication]	--- [None] PAP CHAP MSCHAPV2 EAP-MD5 EAP-TLS	---	Defines the kind of inner authentication for the EAP authentication methods TTLS, PEAP, and FAST.
auth_ano_name [Anonymous name]	max. 64 characters [a-z, A-Z, 0-9]	[blank]	Defines the anonymous name for the unencrypted part of the EAP authentication methods TTLS, PEAP, and FAST.

Parameters	Value	Default	Description
auth_wpa_addon [WPA add-on]	max. 255 characters [a-z, A-Z, 0-9]	[blank]	Specifies an optional WPA expansion.

Table 36: Parameter List - USB device

Parameters	Value	Default	Description
autoSync [Parameter backup]	on/off	on	Enables/disables the automatic parameter backup to a connected USB flash drive.

Table 37: Parameter List – Status page

Parameters	Value	Default	Description
spage [Status page]	on/off	on	Enables/disables the printing of status and service pages on the printer. *The print job can be triggered by pressing the status/reset button on the device or by clicking the corresponding button in the TPR Control Center.*
spMode [Status page mode]	ASCII PostScript DATAMAX Citizen-Z	ASCII	Defines the data format in which the status page is printed.

9.3 Troubleshooting

This chapter describes some problems and their solutions.

Problem

- 'The TPR indicates the BIOS mode' ⇨120
- 'A connection to the TPR Control Center cannot be established' ⇨121
- 'The password is no longer available' ⇨122

The TPR indicates the BIOS mode

Possible Cause

The TPR switches to the BIOS mode if the firmware functions well but the software is faulty. This may happen in the case of an incorrect software update, for example. The TPR indicates the BIOS mode when the activity LED is blinking green.

The TPR is not operational in the BIOS mode.

If the TPR is in the BIOS mode, the filter 'BIOS mode' will be created automatically in the device list of the InterCon-NetTool. The TPR is displayed within this filter.

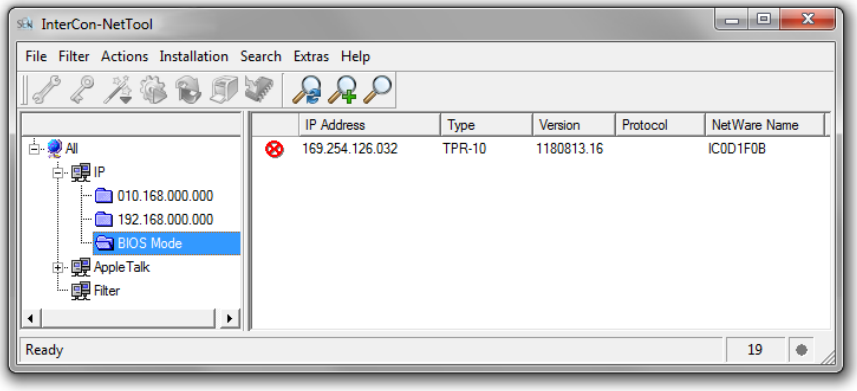


Fig. 7: InterCon-NetTool - TPR in the BIOS Mode

The software must be reloaded to the TPR so that the TPR can switch from the BIOS mode to the normal mode.

Proceed as follows:

1. *Start the InterCon-NetTool.*
2. *Highlight the TPR in the device list.*
   (You will find the TPR under the filter 'BIOS mode'.)
3. *Select* **Installation – IP Wizard** *from the menu bar.*
   The IP Wizard is started.
4. *Follow the instructions of the wizard in order to assign an IP address to the TPR.*
   The IP address is saved.
5. *Carry out a software update on the TPR; see:* ⇨ 90.

The software will be saved in the TPR. The TPR switches to the normal mode.

A connection to the TPR Control Center cannot be established

Eliminate possible error sources. First of all, check:

- the cabling connections,
- the IP address of the TPR (⇨ 13) as well as
- the proxy settings of your browser.

If you still cannot establish any connection, the following safety mechanisms might be the cause:

- ☐ The access is protected via SSL/TLS (HTTPS) ⇨ 63.
- ☐ The TCP port access control is enabled ⇨ 66.
- ☐ The password protection is enabled ⇨ 63.
- ☐ The HTTP port was changed ⇨ 40.
- ☐ The cipher suites of the encryption level are not supported by the browser ⇨ 65.

The password is no longer available

The access to the TPR Control Center can be protected by a password. If the password is no longer available, you can reset the parameter values of the TPR to their default settings to get access to the TPR Control Center ⇨ 87. Previous settings will be deleted.

9.4 List of Figures

TPR Control Center - START 19
InterCon-NetTool - Main Dialog 21
Administration via Email - Example 1 24
Administration via Email - Example 2 24
InterCon-NetTool - IP Wizard 27
TPR Control Center - Certificates 69
InterCon-NetTool - TPR in the BIOS Mode 120

9.5 Index

A

Address
  Ethernet address 98
  Hardware address 98
  IP address 99
  MAC address 98
Administration
  Email 22
  Status/reset button 24
  TPR Control Center 18
ARP/PING 16
Authentication 76
AutoConnect 7

B

Backup copy 83
Bandwidth 50
Bandwidth limit 50
BIOS mode 120
Block port 64
Bonjour 35
BOOTP 14

C

CA certificate 68
Certificate 67
  Create 70
  Delete 75
  Display 70
  Save 72
Certificate request 71
Cipher Suite 61
Connection Service 7

D

Default certificate 68
Default name 97
Default setting 87
Descriptions 38
Device number 97
DHCP 14
DNS (Domain Name Service) 30

E

EAP 76
EAP-FAST 81
EAP-MD5 77
EAP-TLS 77
EAP-TTLS 78
Email 22
Encrypted print data 59
Encryption 45, 59, 61
Encryption Level 61
Ethernet address 98

F

Firmware 90

G

Gateway 98

H

Hardware address 98
Host name 98
Hotline 10
HTTP/HTTPS 63

I

IEEE 802.1x 76
Improper use 11
Intended use 11
InterCon-NetTool 20, 99
  Install 20
  IP Wizard 15
  Start 20

Structure 21
Internal network 38
IP address 99
Local 38
Printer 39
Save 13
IPP connection 51
IPv4 26
IPv6 28

J

Job history 94
Delete 95
Display 94

L

Local service ports 40
LPD protocol 51

M

MAC address 98
Masquerading 39

N

NAT 39, 57
Notification Service 41
Email 42
SNMP Trap 42
Notification service 41
Notifications 41

P

Parameter backup 85
Parameter list 100
Parameters
Default settings 87
Display 84
Load 84
Load automatically 86
Parameter list 100
Save 84
Save automatically 86
Parameters file 83, 85
Password 64
PEAP 80
Personal Printer 6
Personal Printing Client 6
Personal Printing encryption 7, 45
Personal Printing printer 47
Personal Printing server 6
Check identity 46
Configure 44
Ping 54
pkcs(12) 73
POP3 32
Print
Service page 93
Status page 93
Printer
Connection status 54
ID 47, 51
Internal network 39
Messages 56
Transfer method 51
Printer messages 56
Protocol
BOOTP 14
DHCP 14
IPP 51
IPv4 26
IPv6 28
LPD 51
POP3 32
SMTP 33
SNMP 31
SSL/TLS 61
ZeroConf 14

R

RADIUS 76
RAW/socket connection 51
Reset 87

Restart 91
Root certificate 45, 46, 68

S

S/MIME certificate 69
Security 60
Security level 66
SEH Homepage 10
Self-signed certificate 68
Service page 92
  Data format 92
  Print 93
  Printer 92
SMTP 33
SNMP 56
  SNMPv1 31
  SNMPv3 31
SNMP trap 41
SNTP Server 36
Software 90
SSL/TLS encryption
  Personal Printing 45
  ThinPrint 59
Status email 41
Status page 92
  Data format 92
  Print 92
  Printer 92
Status/reset button 24, 88
  Print service page 93
  Print status page 93
  Resetting parameters 88
Subnet mask 99
Support 10
System requirements 7

T

TCP port access control 66
TCP/IP 26
Test mode 66
ThinPrint Client 6
ThinPrint Connection Service 7
  Configuring 57
ThinPrint encryption 7, 59
ThinPrint Engine 6
ThinPrint port 50
Time of the device 36
Time server 36
Time zone 36
TPR Control Center 18, 99
  Language 19
  Start 18
  Structure 19
Transfer methods 51
Types of connection 63

U

Update 90
USB device 85
  Format 86
  Parameter backup 85
UTC 36

V

Version number 90

W

Web access 63
Web connection types
  Define 63

Z

ZeroConf 14